TRABAJO FIN DE MÁSTER EN

SISTEMAS INTELIGENTES

CURSO 2010-2011

ANÁLISIS FORENSE DE IMÁGENES DE MÓVILES MEDIANTE EL USO DE METADATOS

David Manuel Arenas González

Director:

Luis Javier García Villalba

Departamento de Ingeniería del Software e Inteligencia Artificial

Convocatoria: Septiembre de 2011 Calificación: Sobresaliente

MÁSTER EN INVESTIGACIÓN EN INFORMÁTICA

FACULTAD DE INFORMÁTICA

UNIVERSIDAD COMPLUTENSE DE MADRID

Autorización de Difusión

El abajo firmante, matriculado en el Máster en Investigación en Informática de la Facultad de Informática, autoriza a la Universidad Complutense de Madrid (UCM) a difundir y utilizar con fines académicos, no comerciales y mencionando expresamente a su autor el presente Trabajo Fin de Máster: "***Análisis Forense de Imágenes de Móviles Mediante el Uso de Metadatos***", realizado durante el curso académico 2010-2011 bajo la dirección de Luis Javier García Villalba en el Departamento de Ingeniería del Software e Inteligencia Artificial, y a la Biblioteca de la UCM a depositarlo en el Archivo Institucional E-Prints Complutense con el objeto de incrementar la difusión, uso e impacto del trabajo en Internet y garantizar su preservación y acceso a largo plazo.

_____

David Manuel Arenas González

Resumen

Actualmente el número de cámaras fotográficas en dispositivos móviles crece a un ritmo imparable. Asimismo la calidad y prestaciones de las mismas hacen que sean de uso común, desbancando poco a poco a las Cámaras fotográficas digitales. Este escenario produce que el análisis forense de este tipo de imágenes cobre especial importancia y sea necesario y útil en multitud de situaciones (pruebas en casos judiciales, espionaje industrial, privación de la libertad de prensa, pederastia, etc).

Dentro de las diversas ramas del análisis forense, este trabajo se centra en la adquisición de la fuente que produjo la imagen. Para ello se ha desarrollado una técnica que a partir de los metadatos Exif, permite en ciertos casos la obtención de la fuente (marca y modelo) con la que se realizó la fotografía. Asimismo se ha desarrollado una herramienta de ayuda al analista forense que permite diversas funciones complejas que ayudan al analista forense, como son los distintos tipos de consultas avanzadas sobre la información de los metadatos Exif de grandes conjuntos de imágenes o funciones de geoposicionamiento.

Palabras clave

Adquisición de la imagen, identificación de fuente, cámara de teléfonos móviles, Exif, metadatos, análisis forense, métodos forenses, clasificación de fotos.

Abstract

Currently the number of cameras in mobile devices is growing at an unstoppable rate. Also the quality and performance of the same make are in common use, edging slowly to Digital Cameras. This scenario causes the forensic analysis of such images is particularly important and necessary and useful in many situations (pruebas en casos judiciales, espionaje industrial, privación de la libertad de prensa, pederastia, etc.).

Among the various branches of forensic analysis, this paper focuses on the acquisition of the source that produced the image. For this we have developed a technique based on Exif metadata, allows certain cases to obtain the power (make and model) with which the photo was taken. It has also developed a tool to help the forensic analyst allowing various complex functions that help the forensic analyst, such as different types of advanced queries on Exif metadata information of large sets of images or functions of geopositioning.

Keywords

Image adquisition, source identification, camera mobile phones, Exif, metadata, forensics analysis, forensic methods, photo classification.

Lista de acrónimos

A-GPS	Assisted Global Positioning System
BMP	Bit Mapped Picture
CCD	Charge-Copled Device
CFA	Color Filter Array
CIPA	Camera and Imaging Products Association
CMOS	Complementary Metal Oxide Semiconductor
CMY	Cyan-Magenta-Yellow
CYGM	Cyan-Yellow-Green-Magenta
DCF	Design rule for Camera File system
DIP	Digital Image Processor
DSC	Digital Still Camera
EM	Expectation Maximization
EMS	Enhanced Messaging Service
EXIF	Exchangeable Image File Format
GA	Genetic Algorithm
GIF	Graphics Interchange Format
GRGB	Green-Red-Green-Blue
HTML	HyperText Markup Language
IFD	Image File Directory

IIM	Information Interchange Model
IPTC	International Press Telecomunication Council
IPTC-IIM	International Press Telecomunication Council - Information Interchange Model
JEITA	Japan Electronics and Information Technology industries Association
JFIF	JPEG File Interchange Format
JPEG	Joint Photographic Expert Group
KML	Keyhole Markup Language
MMS	Multimedia Messaging System
MP3	MPEG Audio Layer III
MP4	MPEG-4 Part 14
PIL	Python Imaging Library
PNG	Portable Network Graphics
PNU	Pixel Non-Uniformity
PSD	PhotoShop Document
RDF	W3C Resource Description Framework
RGBE	Red-Green-Blue-Emerald
SMS	Short Message Service
SVM	Support Vector Machine

TIFF	Tagged Image File Format
WAV	Waveform Audio Format
XML	Extensible Markup Language
XMP	eXtensible Metadata Platform

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

Actualmente, las ventas de dispositivos móviles (teléfonos, smartphones, PDAs, *tablets*, etc.) siguen aumentando incluso con el impacto de la crisis financiera global. La inmensa mayoría, concretamente el 75% de los teléfonos móviles en 2009, tienen una cámara fotográfica integrada [1]. Las cámaras integradas en dispositivos móviles ya superan en número a las cámaras de fotos tradicionales (DSCs). La previsión de ventas de cámaras fotográficas integradas en dispositivos móviles para 2011 supera los mil millones de unidades y se estima en unos mil trescientos millones de cámaras para 2012 [2]. De igual modo existen predicciones para el futuro que indican que las DSCs desaparecerán en pro de las nuevas integradas en dispositivos móviles [3], ya que el aumento de calidad de estas cámaras crece a un ritmo imparable.

Asimismo no sólo debe medirse en cifras de ventas la irrupción de las cámaras de dispositivos móviles en la sociedad actual. En nuestro día a día es habitual ver como se realizan y usan fotografías de este tipo de dispositivos para una gran diversidad de situaciones (vida personal, noticias, pruebas judiciales, aplicaciones para teléfonos móviles, etc.).

Con los datos anteriores se quiere dar a conocer el continuo crecimiento y la penetración que tienen las cámaras de los dispositivos móviles en nuestro entorno. Este progreso hace que el tratamiento y la toma de fotografías con este tipo de dispositivos puedan crear situaciones problemáticas o beneficiosas en las distintas realidades.

Muchos estiman que este tipo de cámaras facilitan la proliferación de crímenes contra la privacidad y la seguridad de la información (robo con tarjetas de crédito, pornografía infantil, espionaje industrial, etc.). De hecho, una de las principales razones de la existencia hoy en día de dispositivos sin cámaras fotográficas se debe a que diversas compañías, organizaciones o países poseen normas que prohíben o limitan su uso [4]. Un ejemplo de ello es Corea

del Sur, cuya legislación requiere que las cámaras de dispositivos móviles produzcan un sonido cuando realizan la fotografía. En el otro lado existen razones para ver que esta proliferación de las cámaras fotográficas en dispositivos móviles son beneficiosas para las distintas situaciones en las que se requiere una prueba gráfica de un hecho (pruebas criminales o de delitos, privación de la libertad de prensa, etc.).

Por todo ello es necesario proveer a los analistas forenses de herramientas que faciliten su tarea. Dadas las características técnicas particulares de este tipo de fotografías, esta herramienta de análisis forense debería ser específica, no siendo válidas las herramientas que tratan imágenes no generadas por dispositivos móviles.

El resto de este capítulo está organizado de la siguiente forma: el apartado 1.1 presenta el objeto de la investigación de este trabajo, en el apartado 1.2 se analizan los trabajos relacionados más importantes con el objeto de la investigación y finalmente en el apartado 1.3 se resume la estructura del resto del trabajo.

1.1 Objeto de la investigación

El área del análisis forense de imágenes puede dividirse en dos grandes ramas: autenticidad de las imágenes e identificación de la fuente de adquisición de la imagen [5].

Con respecto a la primera de las ramas, nos referimos a determinar si una imagen no ha sufrido ningún procesamiento posterior al de su creación, es decir, que no haya sido manipulada. Los algoritmos forenses utilizados en esta rama deben desvelar ciertas características o trazas que pueden quedar en la imagen al ser manipulada o verificar la integridad de propiedades típicas introducidas en el proceso de adquisición de la imagen.

La segunda de las ramas apunta a la identificación de la fuente de creación

de la imagen. Esta rama se basa en las características del proceso de adquisición del dispositivo concreto y de la tecnología utilizada. Este tipo de algoritmos forenses se basan en el análisis estadístico de los valores de características particulares, las cuales pueden ser entendidas como "marcas de agua naturales e inherentes" a la imagen.

Aún teniendo en cuenta estas dos grandes ramas no se puede dejar pasar por alto la información de los metadatos que los dispositivos introducen en el proceso de adquisición de la fotografía. Suponiendo la veracidad de los datos contenidos en la imagen, es decir, que no se hayan dado manipulaciones mal intencionadas a posteriori, dependiendo de cada fabricante y dispositivo se arroja en una diversidad de formatos, una información útil para el analista forense (localización GPS, fuente de la foto, características técnicas de la imagen, etc.). El análisis estadístico de esta información puede ser de gran utilidad para el analista forense y servir como apoyo para la creación de técnicas de las dos ramas principales anteriormente descritas.

Así, el objeto de esta investigación puede resumirse como la creación de técnicas forenses que permitan identificar la fuente de adquisición de una imagen generada por un dispositivo móvil. Más concretamente, va a centrarse en la obtención de los metadatos de las imágenes y su utilización como técnica de apoyo al análisis forense. Posteriormente, se planteará la necesidad o no de la aplicación, adaptación y creación de algoritmos forenses que permitan la identificación de la fuente basadas en el contenido de la imagen y no en sus metadatos.

1.2 Trabajos relacionados

Las imágenes creadas con móviles presentan características especiales que deben tenerse en cuenta en la elaboración de técnicas y algoritmos para el análisis forense en cualquiera de sus ramas. En [6] [7] se realiza un estudio de los potenciales elementos que pueden ser objeto de análisis forense en

dispositivos móviles.

Existe una gran variedad de trabajos que hacen referencia a los distintos tipos de metadatos en las imágenes con fines de búsquedas y clasificación [8] [9] [10]. En estos trabajos se busca obtener patrones de valores en metadatos para conjuntos de fotografías que puedan arrojar datos válidos para el análisis forense. En lo referente a esta parte es esencial tener en cuenta cuales son los estándares de metadatos utilizados en la industria. El estándar empleado de forma mayoritaria en las cámaras digitales de cualquier tipo es Exif [3]. Aún así es necesario realizar un análisis pormenorizado de otras alternativas como TIFF, JFIF, IPTC y XMP. Independientemente del estándar utilizado, los metadatos tienen un gran problema con respecto al análisis forense: su facilidad de manipulación. Existen aplicaciones que no sólo permiten ver todos los metadatos agregados por los distintos estándares, sino que posibilitan también su edición de una forma gráfica y sencilla. Se puede decir en cierta forma que los metadatos incluidos en las imágenes gozan de una alta "vulnerabilidad".

Una vez estudiado a fondo los metadatos se necesita dar un paso más: técnicas y algoritmos que utilicen el contenido de la propia imagen. Cabe destacar que al igual que ocurre con los metadatos, las imágenes pueden ser modificadas malintencionadamente para evitar o "engañar" las técnicas forenses que se le apliquen. Es decir, estás técnicas y algoritmos son más robustos que las que utilizan los metadatos, ya que se necesitan de conocimientos más profundos para romper el análisis forense que se les realiza, pero son igualmente "vulnerables" [5]. Dentro de este tipo de técnicas y algoritmos, en principio, nos centraremos en las referentes a la identificación de la fuente con la que se realizó la imagen.

Para la creación de estos algoritmos primeramente se necesita tener un amplio conocimiento del proceso de generación de imágenes por parte de este tipo de dispositivos. En [11] se hace una comparativa de cómo difiere el proceso de adquisición de imágenes en cámaras de teléfonos móviles, en DSCs y en escáneres.

Con respecto a la identificación del dispositivo fuente que generó la imagen hay que concretar que el objetivo es obtener la marca del dispositivo y el modelo concreto. Principalmente estas técnicas se basan en analizar las características de la matriz de filtros de color (CFA) y los defectos y no uniformidades en el sensor CCD o CMOS. También es necesario que el algoritmo sea robusto con respecto a las distintas manipulaciones, como por ejemplo la compresión JPEG que realizan este tipo de dispositivos.

Los estudios realizados hasta el momento se dividen básicamente en dos enfoques dependiendo de la información que utilizan [6] [12]. El primer grupo usa el ruido del sensor y la información de la matriz del sensor CCD o CMOS. El segundo grupo tiene en cuenta el proceso de interpolación propio de cada dispositivo que se da a partir de su matriz CFA [13] (también denominado *demosaicing)* y las características inherentes a la imagen [14]. Además de estos dos grandes grupos existen métodos alternativos como el de distorsión radial de la lente (*lens radial distorsion*) [15], características del polvo en el sensor (*sensor dust characteristics*) [16] o el modelo de correlación entre píxeles (*inter-pixel correlation model*) [17].

En [14] se presenta un conjunto de características de las imágenes válidas para el estudio forense, separando éstas en tres grandes grupos: características del color (*color features*), características de la calidad (*quality features*) y características de la imagen en el dominio de la frecuencia (*image characteristics of frequency domain*). Existen referencias concretas sobre el tratamiento de cada conjunto de características [18] [19] [20].

Una vez seleccionada el tipo de información que se va a utilizar o las características a examinar, se ha de elaborar un algoritmo que dada una imagen nos ofrezcan la identificación de la fuente con un grado de confiabilidad lo más alto posible. Existen distintos algoritmos utilizados para DSCs los cuales deben ser objeto de análisis para poder ser adaptados en el futuro al caso concreto que nos ocupa [15] [16] [17] [21] [22] [23] [24] [25] [26] [27] [28].

Asimismo existen ya algoritmos y técnicas específicas para dispositivos móviles [12] [14] [29] [30] que deben ser analizadas para poder ser modificadas con el objetivo de minimizar el porcentaje de error.

1.3 Estructura del trabajo

El resto del trabajo está organizado en 7 capítulos con la estructura que se comenta a continuación.

El capítulo 2 realiza un estado del arte del análisis forense para imágenes generadas por dispositivos móviles. Dentro de este punto se razona en profundidad la necesidad de este tipo de análisis en la sociedad actual. Además se hace un compendio de las principales técnicas utilizadas con sus respectivos resultados.

En el capítulo 3 se realiza una descripción de los principales sistemas de metadatos en imágenes dando una especial importancia al estándar Exif por su alto grado de utilización en imágenes generadas por dispositivos móviles.

En el capítulo 4 se realiza un análisis binario manual de los metadatos de imágenes reales de varios teléfonos móviles. Este análisis permite una comprensión más a fondo del estándar Exif. Sorprendentemente en este análisis se han encontrado fabricantes que violan la especificación Exif de forma sistemática. Se describen algunos de los casos de violaciones encontrados y sus consecuencias.

El capítulo 5 presenta la herramienta desarrollada para la extracción de metadatos Exif de imágenes. Seguidamente se realiza una comparación de la herramienta con otras del mismo segmento.

En el capítulo 6 se realizan diversos análisis sobre un banco propio de imágenes de dispositivos móviles. Para éstos se utiliza la herramienta desarrollada.

Por último, el capítulo 7 muestra las principales conclusiones extraídas de este trabajo así como algunas líneas futuras de trabajo.

En el anexo A se realiza una descripción en profundidad donde se muestran las distintas funcionalidades y la forma de utilizarlas, además de una presentación general del diseño e implementación de la aplicación.

2. ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

2.1. Necesidad de análisis forense en dispositivos móviles

Como se comentó en el capítulo introductorio los dispositivos móviles proliferan a un ritmo imparable en nuestra sociedad. Los avances en las tecnologías de semiconductores permiten que dispositivos móviles amplíen a pasos agigantados su capacidad de procesamiento y almacenamiento. Esto hace que estos dispositivos puedan ser usados como evidencias en procesos judiciales o investigaciones policiales de todo tipo.

A continuación se van a describir casos en los que se aprecia de una forma clara y razonada la necesidad de herramientas para el análisis forense en este tipo de dispositivos [7]: transmisión de información personal y corporativa y transacciones electrónicas.

Con respecto a la transmisión de información personal y corporativa hay que tener en cuenta que las aplicaciones para los dispositivos móviles son desarrolladas en poco tiempo [31]. Procesadores de texto, hojas de cálculo y aplicaciones de bases de datos han sido portadas a dispositivos móviles [32]. Los dispositivos móviles tienen capacidad para almacenar, ver e imprimir documentos electrónicos, transformándose en "oficinas móviles". De igual manera los dispositivos móviles son centro de envíos de mensajes por su capacidad para comunicarse mediantes mensajes (SMS, EMS y MMS) y correos electrónicos. Por tanto hoy en día los dispositivos móviles son fuente de adquisición, tratamiento y almacenamiento de información relevante.

Acerca de la utilización de los dispositivos móviles como centros de transacciones *on-line*, cabe destacar que se pueden realizar operaciones con tratamiento de datos sensibles como por ejemplo transacciones bancarias, comprar en Internet, reservas de vuelos y hoteles, etc.

En el caso concreto del análisis forense de imágenes de dispositivos móviles

no hay duda de la importancia que puede tener su aplicación como prueba en casos civiles o criminales. Dado el gran uso de este tipo de cámaras y las polémicas que suscitan son muchos los debates y normas que prohíben su utilización (empresas, conciertos, centros educativos, cenas y fiestas de negocios, …). La toma de fotografías en escenarios prohibidos puede, en un futuro, necesitar de este tipo de análisis.

2.2. Elementos involucrados en la adquisición y creación de imágenes

El primer paso para poder entender y crear algoritmos forenses de imágenes es conocer con detalle el proceso de adquisición de imágenes en cámaras digitales. Este puede resumirse en el siguiente gráfico:

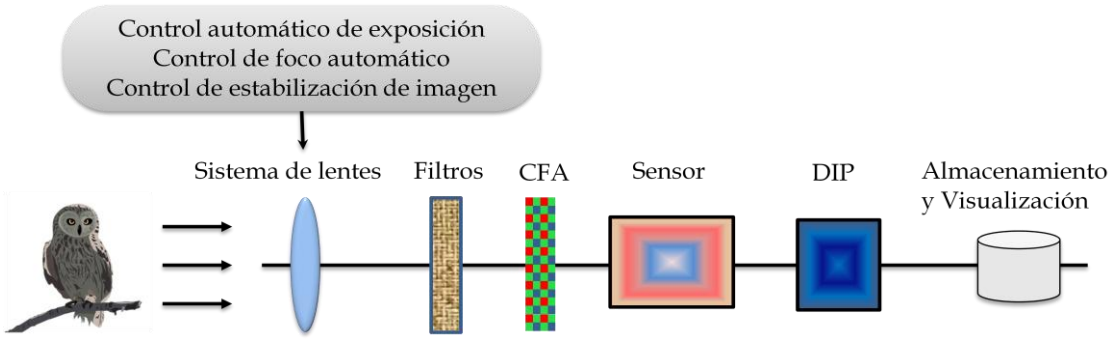


Fig. 1. Proceso de adquisición de imágenes en cámaras digitales

Las cámaras digitales se componen de un sistema de lentes, filtros, matriz de filtros de colores (CFA), sensor de imagen y un procesador digital de imagen (DIP).

Las imágenes a color pueden sufrir aberraciones cromáticas y esféricas causadas por las lentes dado que no existe una lente perfecta. La aberración cromática es la deformidad que se da al converger diferentes longitudes de onda en la misma posición del sensor, mientras que la aberración esférica es un defecto de la lente en el que los rayos de luz que inciden paralelamente al eje óptico, aunque a cierta distancia de éste, son llevados a un foco diferente que los rayos próximos al mismo. En los sistemas actuales de lentes estos efectos son

minimizados por la combinación de lentes cóncavas y convexas. Normalmente el sistema de lentes también posee un control automático de exposición (*auto-exposure*), control de foco automático (*auto-focus*) y una unidad de estabilización de imagen.

Después de pasar a lo largo de las lentes la luz atraviesa un conjunto de filtros. Un filtro infrarrojo absorbe o refleja la luz permitiendo que sólo pase al siguiente filtro la parte del espectro visible, bloqueando la radiación infrarroja que puede hacer decrecer la nitidez de la imagen. Un filtro *anti-aliasing* reduce el *aliasing* (efecto que causa que señales continuas distintas se tornen indistinguibles cuando se muestrean digitalmente). Cuando esto sucede, la señal original no puede ser reconstruida de forma unívoca a partir de la señal digital. El *aliasing* se produce cuando se desea representar una señal de alta resolución en otro medio o forma de resolución menor.

Pasados los filtros se encuentra el verdadero corazón de la cámara digital: el sensor de imagen. Éste es una matriz de foto diodos también denominados habitualmente píxeles. Cuando la luz incide sobre ellos, cada uno genera una señal analógica proporcional a la intensidad de la luz, que es convertida a una señal digital para ser procesada por el DIP. La mayoría de las cámaras utilizan sensores CCD, aunque en los dispositivos móviles es más común el uso de sensores CMOS. Estos píxeles no captan el color, sino el brillo de la luz obteniendo de esta forma una salida monocromática. Para producir una imagen en color se utiliza una matriz de filtros de color (CFA) antes del sensor, por lo que cada foto diodo capta la intensidad de la luz para un solo color (figura 2). La mayoría de las cámaras utilizan el modelo GRGB (Green-Red-Green-Blue) del patrón CFA de Bayer [6]. La salida del sensor con un filtro de Bayer es un mosaico de píxeles rojos, verdes y azules de diferentes intensidades. Ya que cada pixel únicamente almacena uno de los tres colores, la imagen completa es formada por el DIP utilizando distintos algoritmos de interpolación (*demosacing*). Otras alternativas de filtros CFA son el patrón CYGM (*Cyan-Yellow-Green-Magenta*), RGBE (*Red-Green-Blue-Emerald*), CMY (*Cyan-Magenta-*

Yellow). Además de la interpolación el DIP también realiza otros procesamientos auxiliares como el balanceo de blancos (*white balancing*), reducción de ruido (*noise reduction*), definición de la imagen. (*image sharpening*), corrección de la apertura (*aperture correction*) y corrección gamma (*gamma correction*) para producir una imagen final de buena calidad.

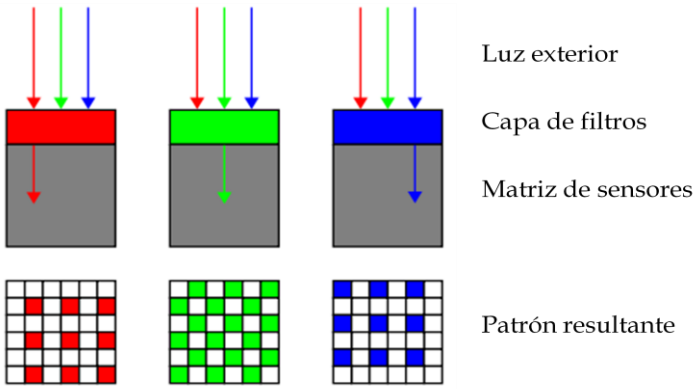


Fig. 2. Matriz de filtros de color (CFA)

2.3. Técnicas de análisis forense de imágenes

En este punto se van a enumerar y describir las principales técnicas de análisis forense para identificar la fuente de la imagen (que es la rama del análisis forense en la que se centra este trabajo). Según [6] se pueden establecer los siguientes cuatro grupos de técnicas para este fin: utilización de la aberración de las lentes, imperfecciones del sensor, interpolación de la matriz CFA y uso de las características de la imagen. Además existe otro grupo de técnicas basadas en los metadatos que constituyen el objeto de este trabajo.

Las anteriores técnicas en su mayoría han sido realizadas teniendo en cuenta las características concretas de las DSCs y no de las cámaras de dispositivos móviles. Algunas de ellas han sido probadas y adaptadas al caso concreto de dispositivos móviles.

2.3.1. Técnicas basadas en la aberración de las lentes

Durante el proceso de adquisición la lente produce aberraciones en la imagen. Existen muchos tipos de aberraciones de la lente como aberración esférica, coma, astigmatismo, curvatura de campo, distorsión radial y distorsión cromática. La distorsión radial es la más grave de todas, especialmente cuando se utilizan lentes gran angular (*wide angle*) baratas.

En [21] se propone la distorsión radial de la lente como la técnica más válida para la identificación de la fuente de la cámara. La distorsión radial produce que las líneas rectas aparezcan como curvas en la imagen. Los autores concluyen que los diferentes fabricantes emplean diseños diferentes de sistemas de lentes para compensar este defecto, por lo que cada modelo de cámara expresará un único patrón de distorsión radial, que ayudará a identificarla.

2.3.2. Técnicas basadas en el uso de las imperfecciones del sensor

Este tipo de técnicas se pueden dividir en dos grandes grupos:

- **Defectos de los píxeles.** En [22] se examinan los defectos de los píxeles del CCD. Dentro de esta técnica se incluye el estudio de los puntos defectuosos (*hot points*), pixeles muertos (*pixel traps*) y defectos de clúster (*cluster defects*). Para investigar sobre los defectos anteriormente enumerados se tomó un par de fotos sobre un fondo totalmente negro con doce tipos de cámaras diferentes. Sobre estas imágenes se hizo una comparación sobre los puntos defectuosos que aparecen como blancos cuando realmente deberían ser negros. El resultado de esta comparación advirtió que cada una de las cámaras tenía un patrón distinto de puntos defectuosos. Sin embargo, también se observó que el número de defectos en los píxeles para una misma cámara difiere entre imágenes y varía mucho dependiendo del contenido de la imagen. También se reveló que el número de defectos de los píxeles varía para el mismo contenido de la imagen y la misma cámara pero tomadas a distintas temperaturas. Asimismo, no se encontraron defectos de pixeles para cámaras con *high-*

end CCD, lo que indica que no todas las cámaras tienen por qué tener este tipo de defectos. Además la mayoría de las cámaras poseen mecanismos adicionales para compensar este tipo de defectos. Se concluye, por tanto, que este método no puede ser aplicado para todas las cámaras digitales.

- **Patrones de ruido del sensor.** En [23] se propone un método utilizando los patrones de ruido del sensor. La no uniformidad de los píxeles (PNU - *Pixel Non-Uniformity*), es decir la diferente sensibilidad a la luz por los píxeles debido a imperfecciones en el proceso de fabricación, es una gran fuente para obtener patrones de ruido. Esto permite que el PNU sea una característica para la identificación unívoca de los distintos sensores y consecuentemente para la identificación de la cámara que posee los mismos. Para el estudio se utilizaron 9 cámaras de las cuales 2 poseían un sensor CCD similar y 2 eran exactamente el mismo modelo. Con este método la identificación de la fuente de la cámara tuvo un 100% de acierto incluso con cámaras con el mismo modelo. De igual manera la identificación fue exitosa para imágenes comprimidas. Aún así, este estudio realizado tiene un problema a destacar, ya que los autores utilizaron el mismo conjunto de imágenes para calcular el patrón de referencia de cada una de las cámaras y para validar el método. En [6] se han realizado pruebas con fotos recortadas y con distintos tamaños de las utilizadas para generar los patrones de referencia y los resultados no han sido satisfactorios.

2.3.3. Técnicas basadas en el proceso de interpolación de la matriz CFA

Dentro de este tipo de técnicas se engloban los siguientes tres grandes grupos:

- **Huellas o trazas en la interpolación del color en las bandas de colores.** En [24] se investiga el proceso de interpolación en la matriz CFA para determinar la estructura de correlación que se utiliza en cada banda de color, que puede ser utilizada con fines de clasificación. La principal

suposición es que el algoritmo de interpolación y el diseño de los patrones de filtros CFA de cada fabricante (incluso de cada modelo de cámara) son algo diferentes entre ellos, lo que hace que resulten distinguibles las estructuras de correlación en las imágenes tomadas. Utilizando el algoritmo de expectativa de maximización (EM), dos conjuntos de características fueron obtenidas para la clasificación de las imágenes: los coeficientes de interpolación de las imágenes y las localizaciones y magnitudes de los picos en el espectro de la frecuencia de los mapas probabilísticos. El estudio determinó que el porcentaje de éxito en la clasificación baja considerablemente cuando el número de cámaras implicadas aumenta. Asimismo esta técnica no es muy buena para cámaras de la misma marca y/o modelo ya que normalmente utilizan patrones de filtros CFA y algoritmos de interpolación similares. De igual modo en el mismo estudio se recalca que no es un buen método para imágenes comprimidas. En [28] se propone un método que introduce mejoras sobre el propuesto en [24], utilizando características adicionales y obteniendo obviamente mejores resultados. Aún así este método sigue estando muy limitado para imágenes con alto grado de compresión.

- **Modelo de correlación cuadrática de píxeles.** En [25] se obtiene una matriz de coeficientes del modelo de correlación cuadrática de píxeles donde la correlación espacial periódica entre píxeles sigue una forma cuadrática. Se probó el método para cuatro cámaras con imágenes de dibujos animados y el éxito fue del 95% para una cámara, del 98% para dos cámaras y del 100% para las restantes dos cámaras. También se realizaron pruebas para imágenes modificadas (entre lo cual se incluye la compresión), con resultados de éxito del 80% para una compresión JPEG del 80%. Para imágenes con otras modificaciones la tasa de acierto es todavía menor. Dado que las cámaras de similar o el mismo modelo utilizan el mismo algoritmo de *demosaicing*, se espera que esta técnica no diferencie correctamente entre distintas cámaras de la misma marca.

Asimismo como prueban los experimentos no es un buen método cuando se tratan imágenes modificadas o comprimidas.

- **Medidas de similitud binarias.** Esta técnica se trata a fondo en [33]. La principal suposición es que los algoritmos de interpolación CFA propietarios dejan correlaciones a lo largo de los planos de bits de una imagen, los cuales pueden ser representados por estas medidas. Las medidas de similitud binarias son métricas utilizadas para medir la semejanza de imágenes binarias, es decir, entre los distintos planos de bits de la imagen. En este estudio se han utilizado 108 medidas de similitud binarias y adicionalmente un conjunto de 10 métricas de calidad de imagen. El mayor porcentaje de éxito para clasificar 3 grupos de cámaras es del 98,7%, mientras que el menor es del 81,3%. Para la clasificación utilizando 9 cámaras, el porcentaje de éxito bajo drásticamente al 62,3%. Claramente se puede apreciar que los resultados de este método dependen del número de cámaras utilizado.

2.3.4. Técnicas basadas en las características de las imágenes

En [26] se identifican un conjunto de características que pueden ser utilizadas para la identificación de la fuente de una imagen. Las 34 características propuestas se han agrupado en 3: características de color, métricas de calidad de la imagen y estadísticas en el dominio *Wavelet*. Estas características fueron extraídas de dos cámaras que han sido utilizadas tanto para el entrenamiento del clasificador como para las pruebas de clasificación. El resultado de acierto es del 98,73% para imágenes sin compresión y del 93,42% para imágenes con compresión JPEG. Este porcentaje baja a 88% cuando se utilizaron cinco cámaras.

En [27] se realizó un estudio similar para diferentes conjuntos de cámaras. El porcentaje de éxito para cámaras con similar sensor CCD es bajo (67,8%). Por lo tanto se concluye que este método es inadecuado para diferenciar cámaras de la misma marca. Asimismo esta técnica requiere que todas las cámaras tomen

imágenes del mismo contenido y resolución lo que, evidentemente, no es nada práctico.

En [29] se utilizó un algoritmo genético (GA) para buscar automáticamente las características óptimas y un clasificador SVM (*Support Vector Machine*) con el objetivo de identificar la fuente de la cámara de distintas imágenes. Los resultados obtenidos son bastante buenos (84% de acierto en el peor de los casos realizado sobre imágenes manipuladas). Además se comprueba la alta robustez de esta técnica frente a distintos tipos de post-procesamiento en las imágenes.

2.3.5. Técnicas basadas en metadatos

Estas técnicas son las más sencillas, aunque dependen en gran medida de los datos que el fabricante decida insertar como metadatos en la imagen en el momento de la toma. Asimismo es este método es el más vulnerable a posibles cambios malintencionados por terceros. Aún así una vez que se pueda comprobar por distintos métodos o situaciones que no ha habido ningún tipo de manipulación externa, el análisis de la gran cantidad de metadatos que, actualmente, como norma general insertan los fabricantes, puede ser de gran ayuda para las funciones del analista forense.

Concretamente, para la identificación de la fuente de la cámara la especificación más seguida por la mayoría de los fabricantes, Exif, cuenta con dos etiquetas concretas *Make* para la marca y *Model* para el modelo. Para la extracción de este tipo de información sólo hay que examinar la especificación a fondo e ir obteniendo los valores de las distintas etiquetas. No es obligatorio que todas las imágenes tengan todos las etiquetas, concretamente las etiquetas *Make* y *Model* pueden no aparecer en el archivo de la imagen. Por tanto, desde el punto de vista de la identificación de la fuente de la imagen si las etiquetas *Make* y *Model* tienen valor, el acierto será del 100% (suponiendo que no ha habido modificación malintencionada) y si no tienen valor, en principio no se puede obtener la fuente con los restantes metadatos. Aún así, el conjunto de los metadatos, con el uso de redes Bayesianas y clasificadores SVM, se ha utilizado

en problemas de clasificación de imágenes [27] (fotografías de interior o exterior, identificación fotografías de puesta de sol y distinción de imágenes creadas por el hombre o tomadas de espacios naturales) .

La extracción de los metadatos puede realizarse con un análisis binario manual o mediante el uso de aplicaciones que analizan la imagen y obtienen un conjunto de todos los metadatos que posee de forma automática.

3. METADATOS EN IMÁGENES

Los metadatos habitualmente son denominados como "datos sobre los datos", es decir, información de interés que complementa el contenido principal de un documento digital. Los metadatos pueden llegar a ser una potente ayuda para la organización y búsqueda a lo largo de librerías de imágenes.

Las imágenes digitales son almacenadas en una gran variedad de formatos como TIFF, JPEG y PSD u otros propietarios como RAW. Cada formato tiene diferentes reglas de cómo cada uno de los formatos de metadatos son almacenados junto al propio archivo que contiene la imagen. Algunos de los distintos contenedores de metadatos para los distintos formatos son: IFDs Exif/TIFF, Adobe XMP e IPTC-IIM. Cada uno de estos contenedores de metadatos tiene un formato propio que indica las propiedades de los metadatos que son almacenados el orden y su codificación en el contenedor. Dentro de cada uno de los contenedores anteriormente comentados suele haber una subdivisión con criterios semánticos, por ejemplo el conjunto de etiquetas GPS en Exif y *Dublin Core* en XMP.

Dentro de cada uno de los grupos semánticos anteriormente referenciados, existe una división en propiedades de metadatos individuales. Cada propiedad tiene asociadas unos tipos de datos específicos como pueden ser cadenas de caracteres, números o vectores. Algunas de esas propiedades son de solo lectura y otras pueden ser modificadas por el usuario. Los metadatos habitualmente contienen información objetiva aunque, en algunos casos, pueden contener información subjetiva. Algunas propiedades como la orientación de la imagen no son comunes a los distintos contenedores estándar; en cambio; otras, como las cadenas *copyright*, pueden ser almacenadas por varios contenedores con similar información pero posiblemente con una semántica u estructura sutilmente distinta (figura 3).

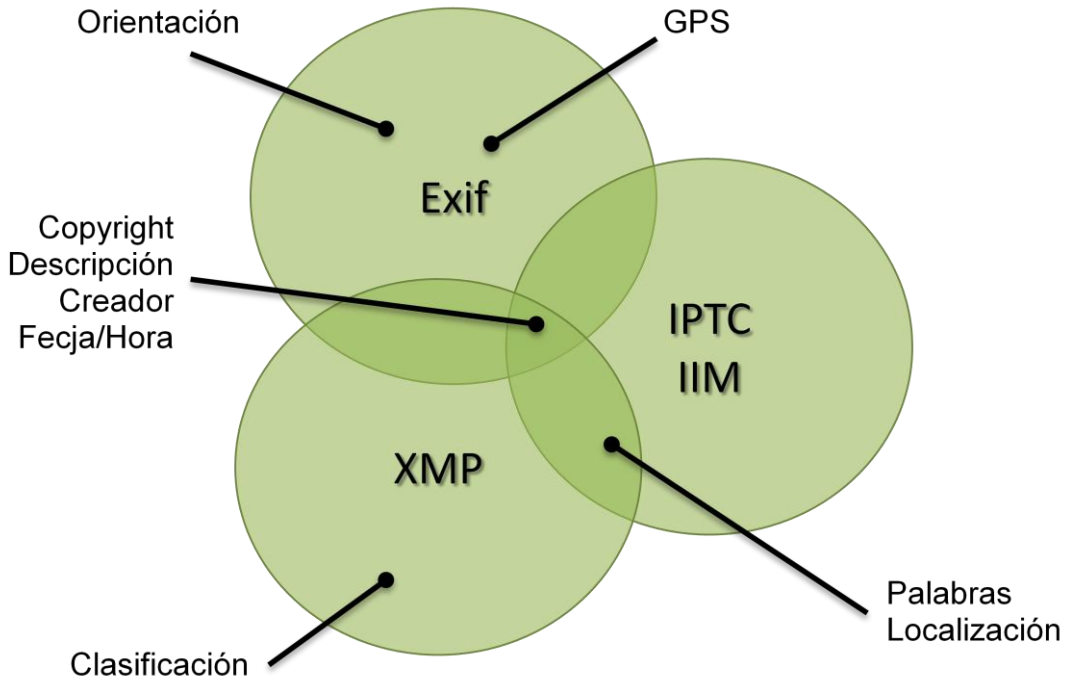


Fig. 3. Contenedores de metadatos

La complejidad estructural descrita anteriormente hace que tradicionalmente cause problemas en el uso eficiente y efectivo de los metadatos. Algunos de los más destacados son:

- Las distintas aplicaciones y dispositivos tratan las especificaciones de metadatos ambiguos o con definiciones incompletas de diferentes formas.
- Las distintas aplicaciones y dispositivos toman diferentes políticas a la hora de almacenar los metadatos que están en distintas localizaciones.
- Las aplicaciones y dispositivos a menudo almacenan metadatos propietarios, denominados *Maker Notes* dentro de los contenedores. Esta práctica es débil y problemática ya que estos datos pueden perderse fácilmente cuando una aplicación diferente modifique el archivo.
- Algunas aplicaciones utilizan las propiedades de forma inadecuada para fines específicos distintos para los que fueron creados. Esto crea problemas de compatibilidad entre las distintas aplicaciones que utilizan

correctamente las propiedades siguiendo las especificaciones establecidas.

- Algunas aplicaciones evitan la complejidad de almacenar los metadatos junto con el archivo de la imagen y optan por separar y almacenar los metadatos en archivos físicos separados. Esto hace que se puedan perder fácilmente los metadatos cuando los archivos de las imágenes son utilizados por distintas aplicaciones.

Todos estos problemas causan en los usuarios frustración y desconfianza sobre los distintos sistemas de metadatos. Los usuarios buscan interoperabilidad entre los distintos productos y servicios de imagen digital. Los fabricantes invierten gran cantidad de recursos para resolver todos estos tipos de problemas. Tanto es así que existen grupos de fabricantes como *Metadata Working Group* [34] con el objetivo de mitigar o erradicar los problemas anteriormente descritos. Este grupo está formado por empresas como Apple, Adobe, Canon, Microsoft, Nokia y Sony. Incluso con la existencia de este grupo, los problemas no se resuelven por completo, dada la inmensa variedad de fabricantes existentes. Cabe destacar que este hecho no implica la inutilidad del uso de metadatos en imágenes, ya que actualmente se puede asegurar que son imprescindibles e inseparables en una imagen digital.

A continuación se describirán en profundidad los estándares y especificaciones de metadatos de imágenes más utilizados en la actualidad, a saber: Exif, TIFF, JFIF, IPTC, XMP.

3.1. Exchangeable Image File Format (Exif)

El estándar Exif (*Exchangeable Image File Format*) ha sido conjuntamente desarrollado por dos asociaciones: JEITA (*Japan Electronics and Information Technology industries Association*) y CIPA (*Camera and Imaging Products Association*). Particularmente, el formato Exif define un conjunto de etiquetas TIFF para describir imágenes fotográficas y es ampliamente utilizado en

cámaras digitales de todo tipo [8]. La especificación usa los formatos de archivos existentes como JPEG y TIFF a los que se agrega etiquetas específicas de metadatos. No está soportado en JPEG 2000 o PNG. Podemos categorizar los metadatos Exif en cuatro grandes categorías [8]:

- Información relacionada con la fecha y hora de diferentes eventos.
- Características técnicas de configuración de la cámara. Ésta incluye información estática como el modelo de cámara y el fabricante, e información que varía con cada imagen como la orientación, apertura, velocidad del obturador, distancia focal y medidor de exposición.
- Información sobre localización, que puede provenir de un GPS conectado a la cámara.
- Descripción e información sobre el *copyright*.

Existen distintas versiones de la especificación Exif. Cada dispositivo soporta una versión la cual incluye a todas las anteriores. Los datos de la versión Exif utilizada son una etiqueta más en los metadatos. Las versiones del estándar son los siguientes:

- Versión 1.0. Octubre de 1995.
- Versión 1.1. Mayo de 1997.
- Versión 2.0. Noviembre de 1997.
- Versión 2.1. Diciembre de 1998.
- Versión 2.2. Abril de 2002.
- Versión 2.21. Septiembre de 2003.
- Versión 2.3. Abril de 2010.

Antes de comenzar a describir con más profundidad la estructura de Exif cabe destacar la existencia de la especificación DCF (*Design rule for Camera File system*) que tiene relación con Exif, además de haber sido también creada por la JEITA. El objetivo de DCF es intentar simplificar el intercambio de archivos entre DSCs y otros equipos. Así, define un conjunto de reglas de almacenamiento, lectura y escritura de los archivos de las imágenes y otros archivos relacionados utilizados por las DCSs. Entre otras cosas, DCF define un subconjunto de Exif, donde algunas de las propiedades son opcionales en Exif pero obligatorias en DCF. Actualmente, DCF es el estándar de facto utilizado en la industria de las cámaras digitales.

Dado que el formato más utilizado en cámaras digitales, y concretamente en dispositivos móviles, es JPEG, a continuación se va a realizar una descripción más detallada de los elementos y estructuras de datos que utiliza JPEG/Exif.

3.1.1. Estructura general del formato JPEG

Inicialmente hay que señalar que todos los archivos JPEG comienzan con el valor binario '0xFFD8' SOI (*Start Of Image*) y terminan con el valor binario '0xFFD9' EOI (*End Of Image*). SOI y EOI son dos marcadores especiales sin datos posteriores. En cambio, todas las marcas salvo las dos anteriores contienen una estructura fija y datos. El formato básico de una marca se muestra en la tabla 1.

0xFF	**Número de marca (1 byte)**	**Tamaño de los datos (2 bytes)**	**Datos (n bytes)**

Tabla 1. Formato básico de una marca

El campo tamaño de los datos sigue la alineación de bytes denominada "Motorola" (*big-endian*), es decir, la lectura comienza por los bits de peso más altos a los más bajos. Por ejemplo, '0xAB21' como tamaño de datos indica que son 43809 bytes. Es importante destacar que en el tamaño de los datos los dos bytes que indican el propio tamaño de los datos están incluidos. Por ejemplo, el

marcador '0xFFC1000C' indica que la marca '0xFFC1' tiene '0x000C' bytes de datos, es decir, 12 bytes de datos. Pero en esos 12 bytes se incluyen los dos bytes que indican el tamaño de los datos. Por tanto, el campo datos tiene una longitud de 10 bytes. Los datos son los 10 bytes siguientes a '0x000C'.

En el formato JPEG existe una marca especial para describir los datos del contenido de la imagen. Esta marca es '0xFFDA' y se denomina SOS (*Start of Stream*). Tras la marca SOS se encuentran los datos propiamente dichos de la imagen y se termina en la marca especial EOI (*End Of Image*). Un esquema general con la posibilidad de marcadores para metadatos (por ejemplo Exif) para una imagen JPEG se presenta en la tabla 2.

SOI	**Marker XX Tamaño=SSSS**			**Marker YY Tamaño=TTTT**			**SOS Tamaño=UUUU**			**Datos Imagen**	**EOI**
FFD8	FFXX	SSSS	Datos	FFYY	TTTT	Datos	FFDA	UUUU	Datos	IIII	FFD9

Tabla 2. Esquema general con marcadores de una imagen JPEG

3.1.2. Estructura de datos Exif

Una vez vista la estructura general a grandes rasgos de un archivo JPEG se va a pasar a un grado más de concreción para llegar a mostrar donde se encuentran ubicados los datos Exif. La estructura general de un archivo JPEG/Exif se encuentra en la tabla 3 (los segmentos obligatorios están marcados con gris).

SOI	Start of Image
APP1 (no excede 64Kb)	Application Marker Segment 1 (Exif Attribute Information)
APP2 (debe ser almacenado en esta posición si es necesario y puede haber varios)	Application Marker Segment 2 (FlashPix Extension Data)
APPn (no son utilizados por Exif, n valor entre 3 y 15 (incluidos))	Application Marker Segment n
DQT	Define Quantization Table
DHT	Define Huffman Table
DRI	Define Restart Interoperability
SOF	Start of Frame
SOS	Start of Scan
Datos de la imagen	Datos comprimidos de la imagen
EOI	End of Image

Tabla 3. Estructura general de un archivo JPEG/Exif

La información Exif es albergada en el segmento APP1. Los segmentos APPn no son utilizados por Exif, pero la especificación no prohíbe su utilización. Pueden ser utilizados por tanto para almacenar cualquier otro tipo información por parte de los fabricantes, que deben velar por mantener la compatibilidad con Exif. El orden de los segmentos DQT, DHT, DRI y SOF es intercambiable.

Exif utiliza un marcador llamado "APP1" (*Application Marker 1*), para evitar conflictos con el marcador APP0 del formato JFIF. Por tanto toda imagen JPEG/Exif comienza con la estructura de la tabla 4.

SOI	**APP1**	**Datos APP1**	**Otros marcadores**
FFD8	FFE1	SSSS 457869660000 TTTT...	FFXX SSSS DDDD...

Tabla 4. Estructura general del marcador APP1 de una imagen JPEG/Exif

Toda la información relacionada con Exif está almacenada en el marcador

APP1. Conviene recordar que el tamaño SSSS de APP1 incluye los dos bytes utilizados para indicar el tamaño. Tras el tamaño SSSS del segmento APP1, existe una cadena para determinar si se sigue el formato Exif o no. La cadena "Exif" en caracteres ASCII ('0x45786966') seguida de 2 bytes '0x00' indican que se está utilizando Exif. Tras el marcador APP1, podrán existir otros marcadores JPEG. La estructura básica del segmento APP1 se presenta en la tabla 5.

APP1 Marker
APP1 Length
Exif Identifier Code
TIFF Header
0th IFD
0th IFD Value
1st IFD
1st IFD Value
1st IFD Image Data

Tabla 5. Estructura general del segmento APP1 de una imagen JPEG/Exif

Los datos APP1 no exceden el tamaño de 64 KB. Tras el indicador de que los datos almacenados en APP1 son Exif, el propio Exif utiliza el formato TIFF para almacenar los datos. Los datos de los atributos están almacenados en la estructura TIFF, que tiene un máximo de dos IFDs (*0th IFD* y *1st IFD*). El *0th IFD* contiene información sobre la propia imagen y el *1st IFD* se utiliza para almacenar todo lo relacionado con la imagen *thumbnail* (imagen en miniatura).

Por tanto tras el indicador "Exif" (con sus dos bytes a '0x00' posteriores) vienen los datos de cabecera TIFF (primeros 8 bytes del formato), que tienen la siguiente estructura:

- Definición del tipo de alineación de los datos. Lo definen los dos primeros bytes. Este dato es de muy importante y siempre tiene que ser tenido en

cuenta. Existen dos opciones:

- 0x4949="II". Alineación *Intel*, es decir alineación *Little Endian*. Por ejemplo el valor 232167 que en decimal es '0x038AE7' en hexadecimal, en este tipo de alineación se almacenaría como '0x03-0x8A-0xE7'.

- 0x4D4D="MM". Alineación *Motorola*, es decir *Big Endian*. Por ejemplo el valor 232167 en decimal es '0x038AE7' en hexadecimal, en este tipo de alineación se almacenaría '0xE7-0x8A-0x03'.

Aunque JPEG siempre utiliza la alineación *Motorola*, Exif permite los dos tipos de alineaciones.

- Los siguientes dos bytes siempre tienen un valor fijo '0x2A00'. Es importante recordar que hay que tener en cuenta el tipo de alineación. Si es "MM" se almacenarían como '0x2A00' y si es "II" como '0x002A'.

- Los últimos 4 bytes de la cabecera TIFF indican el desplazamiento (*offset*) al primer IFD (*Image File Directory*) cuya estructura se definirá posteriormente. Este desplazamiento se cuenta a partir del primer byte del tipo de alineación. Habitualmente el primer IFD comienza inmediatamente después de la cabecera TIFF, por lo que el valor suele ser '0x00000008'.

Un esquema general de la cabecera TIFF se puede observar en la tabla 6.

Alineación (2 bytes)	**Marca fija (2 bytes)**	**Desplazamiento al primer IFD (4 bytes)**
"II" o "MM"	0x2A00	0xLLLLLLLL

Tabla 6. Esquema general de la cabecera TIFF

3.1.2.1. *Image File Directory*

Un IFD (*Image File Directory*) está compuesto por los siguientes campos: 2 bytes

que indican el número de entradas del directorio, entradas del directorio con un tamaño de 12 bytes y un desplazamiento de 4 bytes al siguiente IFD. Por tanto la estructura básica de un IFD se muestra en la tabla 7.

Nº Entradas (2 bytes)	**Entradas del directorio (0xYYYYXXXXNNNNNNNNDDDDDDDD) (12 bytes * 0xTTTT)**				**Desplazamiento al siguiente IFD (4 bytes)**
0xTTTT	Etiqueta (2 bytes)	Tipo de datos (2 bytes)	Nº de elementos (4 bytes)	Valor del desplazamiento (4 bytes)	0xLLLLLLLL

Tabla 7. Estructura básica de un IFD

Cada entrada del directorio (12 bytes) tiene la siguiente estructura:

- **Etiqueta**: Son los dos primeros bytes. Los identificadores de las etiquetas en Exif *0th IFD* y *1st IFD* son los mismos que los de la especificación TIFF. El orden de las etiquetas en un directorio no está especificado en Exif.
- **Tipos de datos**: Siguientes dos bytes. En Exif 2.3 [35] los tipos de datos son:
  - Tipo 1. BYTE. Entero sin signo de 8-bits (1 byte).
  - Tipo 2. ASCII. Un byte (8 bits) que contienen caracteres ASCII de 7 bits. Esta cadena es terminada en NULL (0x00).
  - Tipo 3. SHORT. Entero sin signo de 16 bits (2 bytes).
  - Tipo 4. LONG. Entero sin singo de 32 bits (4 bytes).
  - Tipo 5. RATIONAL. Dos LONGs. El primero es el numerador y el segundo es el denominador. Por tanto este tipo ocupa 64 bits (8 bytes).
  - Tipo 7. UNDEFINED. Tipo byte que puede tomar cualquier valor dependiendo de la definición o significado del campo.

- Tipo 8. SLONG. Un entero con signo de 32 bits (4 bytes) en notación complemento a 2.

- Tipo 9. SRATIONAL. Dos SLONGs. El primero es el numerador y el segundo es el denominador. Por tanto este tipo de dato ocupa 64 bits (8 bytes).

- **Número de elementos**: Siguientes 4 bytes. Indica el número de elementos que almacena la etiqueta. Es muy importante destacar que el número de elementos es algo totalmente diferente al número de bytes. Por ejemplo, si este campo fuera '0x00000004' y el tipo fuera LONG, en los datos se almacenarían 4 LONGs, con lo cual la longitud sería 16 bytes y no 4 (del '0x00000004').

- **Valor del desplazamiento**: Siguientes 4 bytes. Si el valor es '0x00000000' quiere decir que es el último IFD. En este campo hay que tener en cuenta dos casos:

  - Si el tamaño de los datos a almacenar es menor o igual a 4 bytes, este campo almacena directamente los datos.

  - Si el tamaño de los datos a almacenar es mayor de 4 bytes, este campo almacena el desplazamiento donde se encuentran los datos con respecto al comienzo de la cabecera TIFF.

3.1.3. Información *thumbnail*

El formato Exif permite que el archivo contenga una imagen de *thumbnail*, es decir, una imagen en miniatura utilizada para la indexación de la imagen principal. La propia especificación Exif 2.3 no obliga a que todas las imágenes tengan *thumbnail*, pero sí lo recomienda. Esta imagen puede estar en algún formato comprimido o descomprimido independientemente de que el formato de la imagen principal sea comprimido (JPEG). El *thumbnail* se incluye en el *1st*

*IF*D de distinta forma dependiendo de si se almacena en un formato comprimido o descomprimido. Para evitar duplicar definiciones, el *1st IFD* no se utiliza para almacenar etiquetas que posean información TIFF de la imagen o información guardada en otra parte como si fuera cualquier otro marcador JPEG.

3.2. *Tagged Image File Format*

TIFF (*Tagged Image File Format*) es un formato de archivo basado en etiquetas para el almacenamiento e intercambio de imágenes [36]. La primera versión de la especificación TIFF fue publicada por la Corporación Aldus en otoño de 1986, tras una serie de encuentros con una serie de desarrolladores software y fabricantes de escáneres, aunque su versión más reciente es TIFF 6.0 publicada en 1992 por Adobe Systems, que es el actual responsable de la especificación. El propósito de TIFF es describir y almacenar datos de la imagen para proporcionar un entorno rico, con el que las aplicaciones puedan intercambiar datos de la misma.

Los metadatos son un componente esencial del formato TIFF. Los metadatos TIFF se componen básicamente de tres grupos de etiquetas: *Baseline*, *Extension* y *Private*. El conjunto de metadatos TIFF es extensible para propósitos particulares mediante etiquetas privadas. Uno de los conjuntos de etiquetas privadas más destacados son los Exif, formato de metadatos que se ha descrito anteriormente.

Aunque el sistema de metadatos TIFF ha tenido mucho éxito, la proliferación de conjuntos de etiquetas privadas nuevos complica la extracción de los metadatos. Muchos de los programas para extraer metadatos TIFF sólo obtienen las etiquetas pertenecientes a los grupos *Baseline* y *Extension*. Dentro de las etiquetas privados únicamente el conjunto Exif es ampliamente soportado y utilizado por los distintos fabricantes y aplicaciones.

Otras de las características más relevantes de TIFF son:

- TIFF incluye varios esquemas de compresión, que permiten a los desarrolladores elegir el más apropiado para sus aplicaciones.
- No está unido a dispositivos electrónicos específicos.
- Es portable, no favoreciendo a un sistema operativo particular ni a un sistema de archivos, compilador o procesador concreto.
- Está diseñado para ser ampliable y evolucionar según las nuevas necesidades lo requieran.

3.3. *JPEG File Interchange Fomat*

JFIF (*JPEG File Interchange Fomat*) es un formato de archivos de imagen estándar, que contienen las imágenes guardadas en compresión JPEG [37]. Permite el intercambio de metadatos entre una gran variedad de plataformas y aplicaciones. Es un formato simple cuyo único objetivo es el intercambio de imágenes comprimidas JPEG. No incluye algunas de las características avanzadas de otros formatos de archivo de intercambio de imágenes.

Formalmente los estándares Exif y JFIF son incompatibles, ya que ambos especifican que sus segmentos de aplicación deben de ir los primeros en el archivo de imagen. En la práctica muchas aplicaciones producen archivos con ambos segmentos, pero esto puede crear problemas.

3.4. *International Press Telecomunication Council*

IPTC (*International Press Telecomunication Council*) [38], con sede en Londres, es un consorcio de grandes agencias de noticias y publicidad. Ha desarrollado y mantienen un estándar técnico para mejorar el intercambio de noticias. En 1979, el primer estándar del IPTC era solo texto y fue definido para proteger los

intereses de la industria de las telecomunicaciones. Después, en 1991, un nuevo estándar, el IIM (*Information Interchange Model*) fue creado. IMM es un formato para transmitir documentos de noticias en texto, fotografías y otros tipos de archivos multimedia. El IMM define las llamadas cabeceras IPTC, que actualmente existen en gran cantidad de archivos de imágenes. Estas cabeceras tienen una compleja estructura de datos donde se almacena un conjunto de definiciones de metadatos. Estas cabeceras son insertadas por software como por ejemplo Adobe Photoshop.

La información IPTC se encuentra separada en distintos registros cada uno de los cuales tienen sus propias etiquetas. Los registros IPTC son: *IPTC EnvelopeRecord*, *IPTC ApplicationRecord*, *IPTC NewsPhoto*, *IPTC PreObjectData*, *IPTC ObjectData* e *IPTC PostObjectData*.

Adobe creó XMP en 2001 y los estándares IPTC adoptaron XMP como sucesor del IMM en 2005. Éste es ampliamente utilizado por los profesionales de la imagen digital. Información como el nombre del fotógrafo, título de la imagen, información de *copyright*, etc., pueden ser incluidas de forma manual o automática.

3.5. *Extensible Metadata Platform*

XMP (*Extensible Metadata Platform*) [39] es una tecnología de etiquetado basada en XML que permite incluir metadatos en el propio archivo. Con XMP las aplicaciones de escritorio y sistemas de publicidad poseen un método para capturar y compartir información aprovechando los metadatos insertados. XMP estandariza la definición, creación y el procesamiento de los metadatos.

XMP define un modelo de metadatos que puede ser utilizado con cualquier otro conjunto de metadatos definido. XMP también define un particular esquema de propiedades básicas muy útiles para el almacenamiento de la historia de un recurso así como de su procesamiento.

Para el almacenamiento de los datos utiliza un subconjunto del *W3C Resource Description Framework* (RDF). Sin embargo, los usuarios pueden definir sus propias propiedades, es decir, XMP permite a cada programa o dispositivo a lo largo de la vida del archivo añadir su propia información.

Los metadatos XMP son más flexibles que los demás y se adaptan a más usuarios. Se apoyan en los *Dublin Core*. Éstos se componen de un conjunto de 15 elementos. Originalmente, se concibieron para la descripción generada por el autor de recursos en la web, pero se emplean también en bibliotecas y museos. Se crearon los IPTC Core para facilitar la transición de IPTC/IIM hacia XMP. El IPTC Core es una transferencia explícita de los valores de los metadatos de las cabeceras IPTC al marco de trabajo XMP. Pocos programas pueden visualizar los metadatos XMP.

XMP puede ser utilizado en diversos formatos de archivos como PDF, JPEG, JPEG 2000, GIF, PNG, HTML, TIFF, *Adobe Illustrator*, PSD, MP3, MP4, *Audio Video Interleave*, WAV, RF64, *Audio Interchange File Format*, *PostScript*, *Encapsulated PostScript*. En un archivo JPEG la información XMP suele ser incluida junto los metadatos Exif e IPTC.

4. ANÁLISIS BINARIO DE IMÁGENES DE DISPOSITIVOS MÓVILES

Una vez presentada la especificación Exif y teniendo en cuenta que es la utilizada en la mayoría de los dispositivos móviles y DSCs [8], se ha estimado oportuno realizar un análisis manual a nivel binario de imágenes de dispositivos móviles al azar. Este análisis preliminar tiene como objetivos profundizar en el conocimiento de la propia especificación y comprobar si ésta es seguida por los fabricantes.

Obviamente dado el alto número de etiquetas o campos que posee Exif y que cada imagen sólo posee un subconjunto de ellos, se han ido eligiendo algunas estructuras y etiquetas para el análisis, teniendo en cuenta su importancia o la validez para servir como ejemplos de otras parecidas. El análisis ha seguido un orden lógico de estructuras de mayor a menor nivel (estructura general JPEG, cabecera TIFF, marcadores, IFD y etiquetas concretas).

Para un primer análisis se ha tomado azarosamente una imagen de un teléfono móvil Samsung Galaxy S y de un Sony Ericsson W580i. Cabe destacar que estas imágenes han sido tomadas por dispositivos de nuestra propiedad y que no han sufrido ningún tipo de cambio, ni siquiera el nombre del archivo. El formato de las imágenes tomadas es JPEG.

Inicialmente se va a comprobar que los archivos son realmente JPEG a grandes rasgos su estructura general. Es decir, comienzan con el valor binario '0xFFD8' (*SOI Start Of Image*) y terminan con el valor binario '0xFFD9' EOI (*End Of Image*). SOI y EOI son dos marcadores especiales sin datos posteriores. En las figuras 4, 5, 6 y 7 se aprecia que las imágenes cumplen con lo descrito anteriormente.

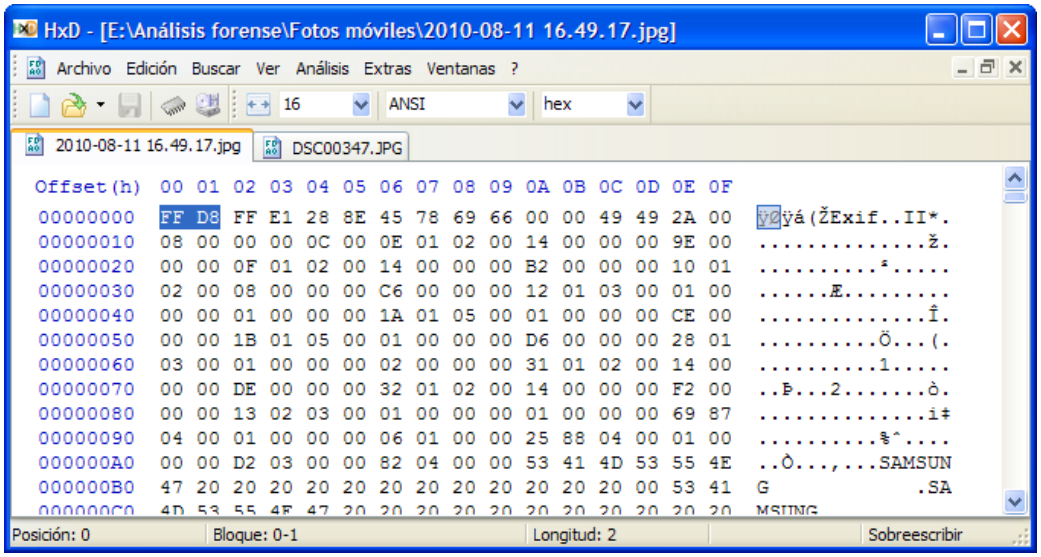


Fig. 4. Ejemplo de *Start Of Image* para Samsung Galaxy S

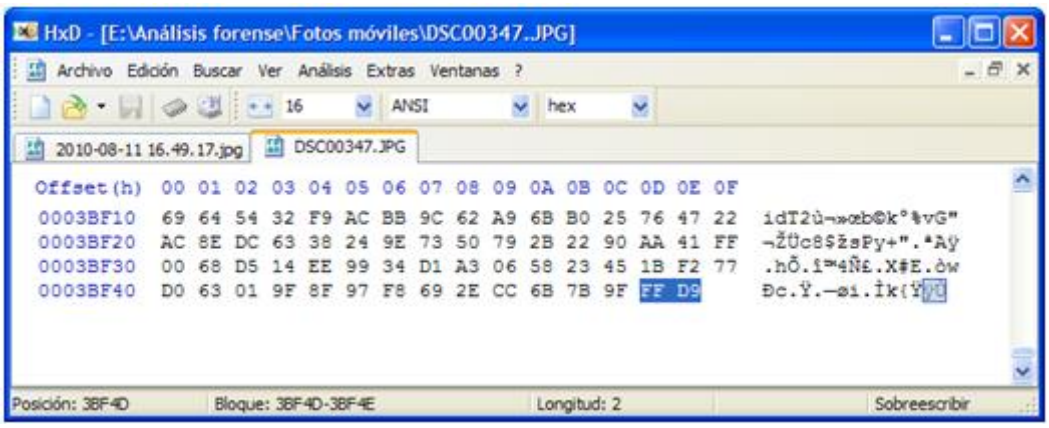


Fig. 5. Ejemplo de *End Of Image* para Samsung Galaxy S

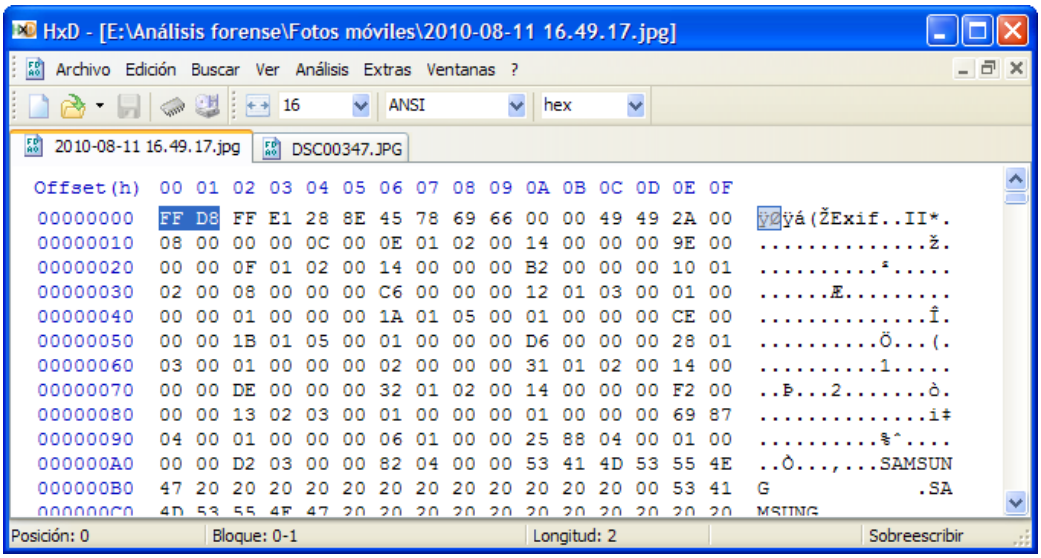


Fig. 6. Ejemplo de *Start Of Image* para Sony Ericsson W580i

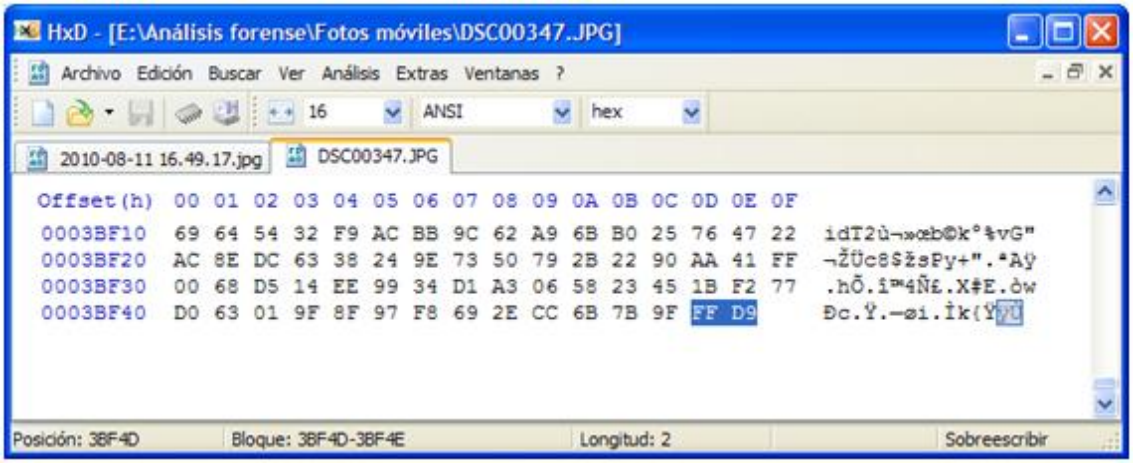


Fig. 7. Ejemplo de *End Of Image* para Sony Ericsson W580i

Tras comprobar que las dos imágenes son JPEG se van a comprobar los datos de la cabecera TIFF. En la figura 8 se observa que para el Samsung Galaxy S los datos de la alineación son Intel ("II") y desplazamiento '0x00000008' al primer IFD.

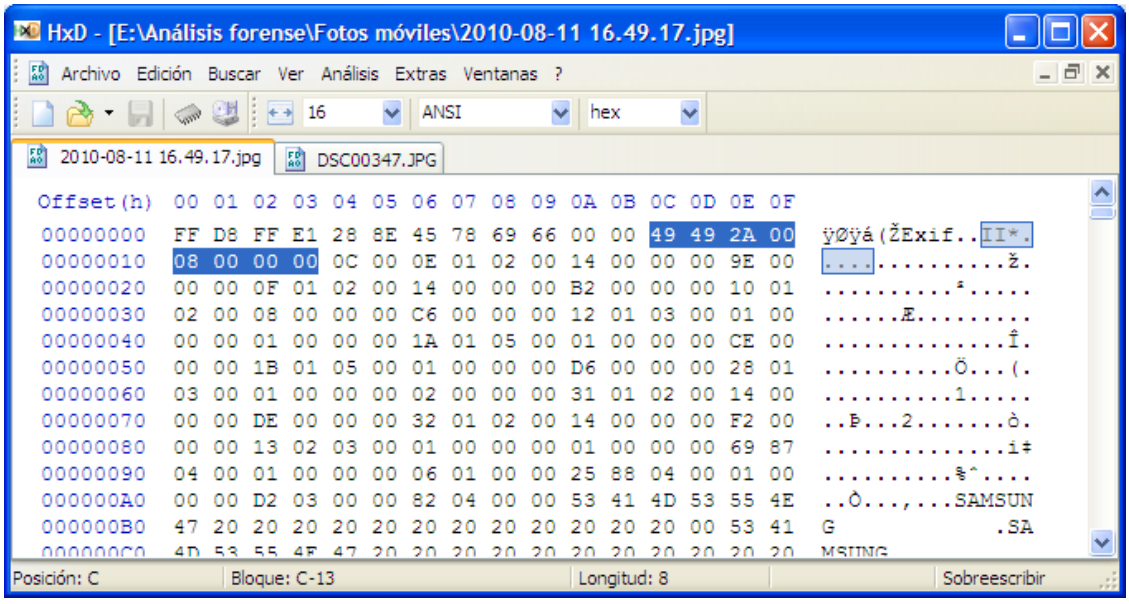


Fig. 8. Ejemplo de la estructura de la cabecera TIFF para Samsung Galaxy S

En la figura 9 se observa que para el Sony Ericsson W580i los datos de alineación son Intel ("II") y desplazamiento 0x00000008 al primer IFD.

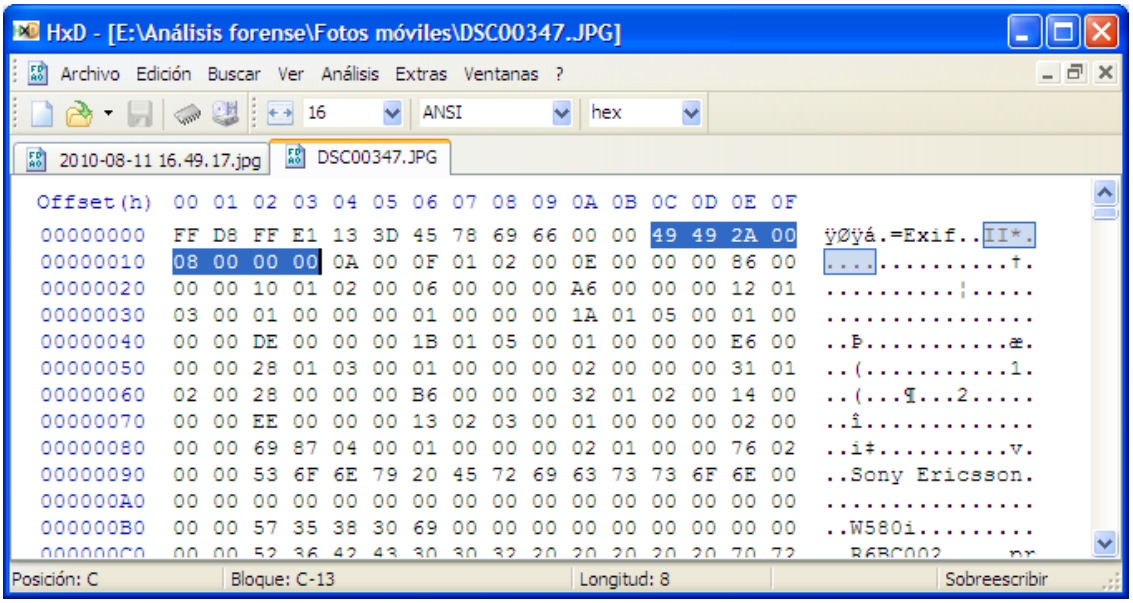


Fig. 9. Ejemplo de la estructura de la cabecera TIFF para Sony Ericsson W580i

Seguidamente se va a analizar la estructura de un marcador concreto: el segmento APP1. Para la imagen del Samsung Galaxy S puede comprobarse en la figura 10 la existencia el marcador APP1 ('0xFFE1'), seguido de su tamaño '0x288E' (alineación "Motorola"), es decir, 10882 bytes de datos (incluidos los 2 bytes que indican la longitud). Por tanto, APP1 en este caso comienza en '0x0004' y termina en '0x2892' (este byte no incluido).

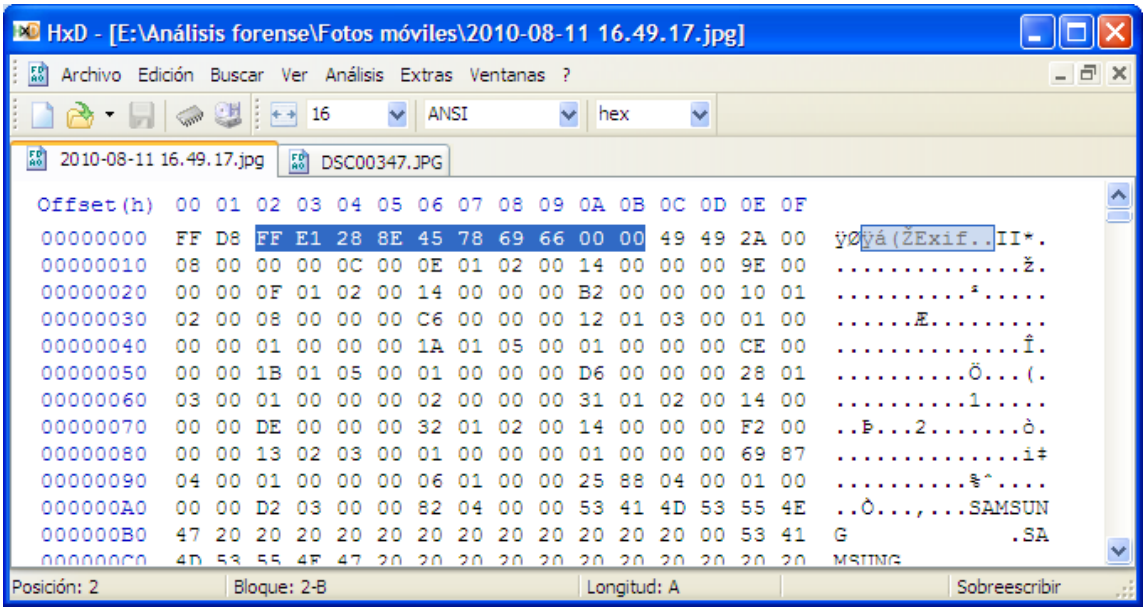


Fig. 10. Ejemplo de la estructura del segmento APP1 para Samsung Galaxy S

Para el caso del Sony Ericsson W580i, igualmente se contempla el marcador APP1 ('0xFFE1') seguido del tamaño '0x133D' (alineación "Motorola"), es decir, 4925 bytes de datos (incluidos los 2 bytes que indican la longitud). Por tanto, APP1 en este caso comienza en '0x0004 y termina en '0x1341' (este byte no incluido) como se puede ver en la figura 11.

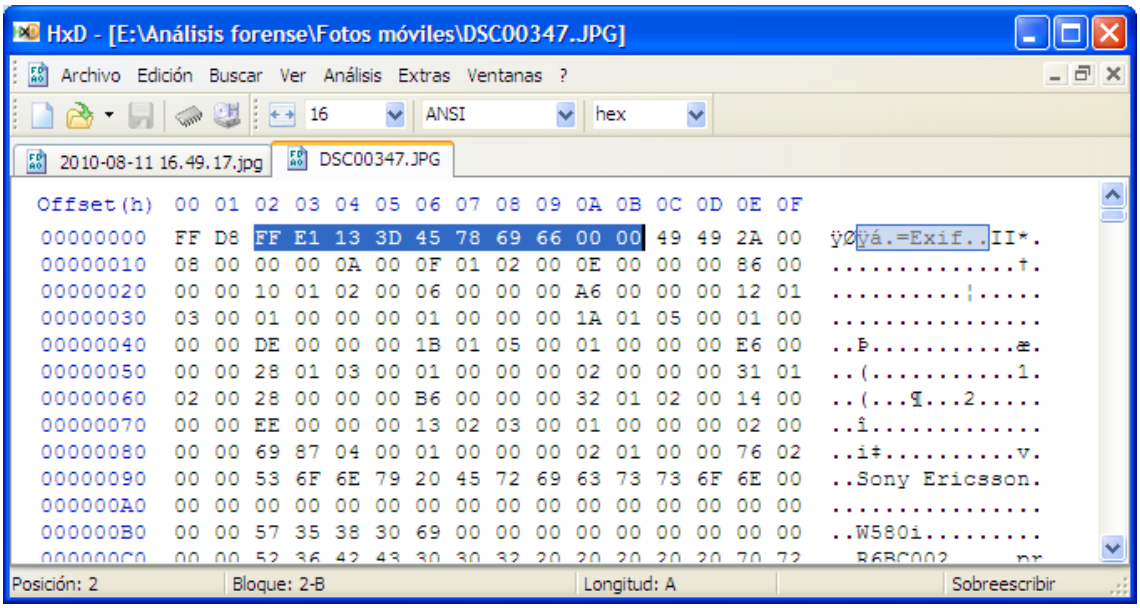


Fig. 11. Ejemplo de la estructura del segmento APP1 para Sony Ericsson W580i

Si se extrae para las dos imágenes el siguiente marcador de APP1 se observan diferentes resultados:

- **Samsung Galaxy S**: El siguiente marcador (en la dirección '0x2892') es '0xFFDB', que según Exif se corresponde con DQT (*Define Quantization Table*).

- **Sony Ericsson W580i**: El siguiente marcador (en la dirección '0x1314') es '0xFFC4', que según Exif se corresponde con DHT (*Define Huffmann Table*).

Con estos dos datos anteriores se observa que, tras APP1, en imágenes diferentes le siguen marcadores diferentes, que es totalmente permitido por Exif.

Una vez analizados algunos marcadores hay que pasar al siguiente nivel: los IFDs. En la imagen del Samsung Galaxy S se va a examinar la estructura de su primer IFD y los dos primeras etiquetas. Tras la cabecera TIFF se encuentran los bytes '0x0C000E0102001400000009E000000'. Teniendo en cuenta siempre que la alineación es "Intel" ("II") los dos primeros bytes '0x0C00' indican cuantas entradas tiene el directorio actual, que es el directorio "0th IFD", ya que es el primero. Por tanto, el "0th IFD" tiene '0x000C' entradas, es decir, 12 entradas, como se puede ver en la figura 12.

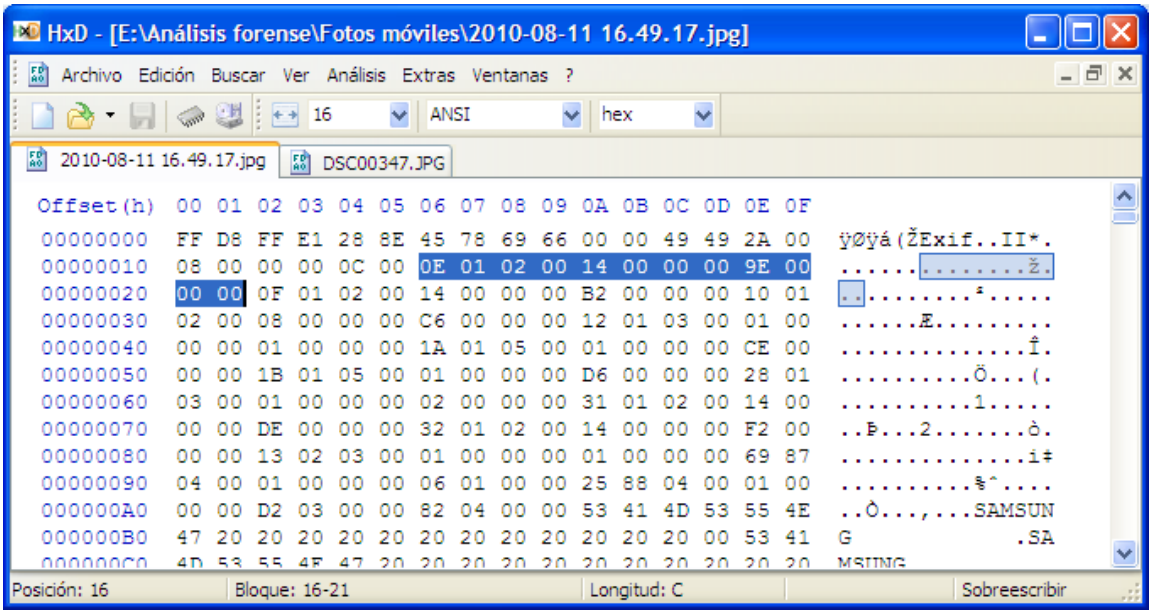


Fig. 12. Ejemplo de la primera entrada del "0th IFD" para Samsumg Galaxy S

En la imagen anterior, se resaltan también en azul la primera entrada del directorio '0x0E0102001400000009E000000', la cual se interpreta de la siguiente forma:

- Etiqueta. 0x010E. etiqueta *Image Description*.
- Tipo. 0x0002. ASCII.
- Número de elementos. '0x00000014', es decir, 20 elementos.
- Desplazamiento. '0x0000009E' con respecto el inicio de la cabecera TIFF, es

decir, 158 bytes.

Por tanto para obtener el valor de la etiqueta *Image Description* (ya que su tamaño es mayor de 4 bytes) tenemos que ir al lugar que nos indica el desplazamiento. En la misma figura se puede apreciar abajo que la longitud es '0x9E' con respecto al inicio de la cabecera TIFF. Por lo que el inicio de los datos de la etiqueta comienza por tanto en la posición '0xAA' (ver figura 13).

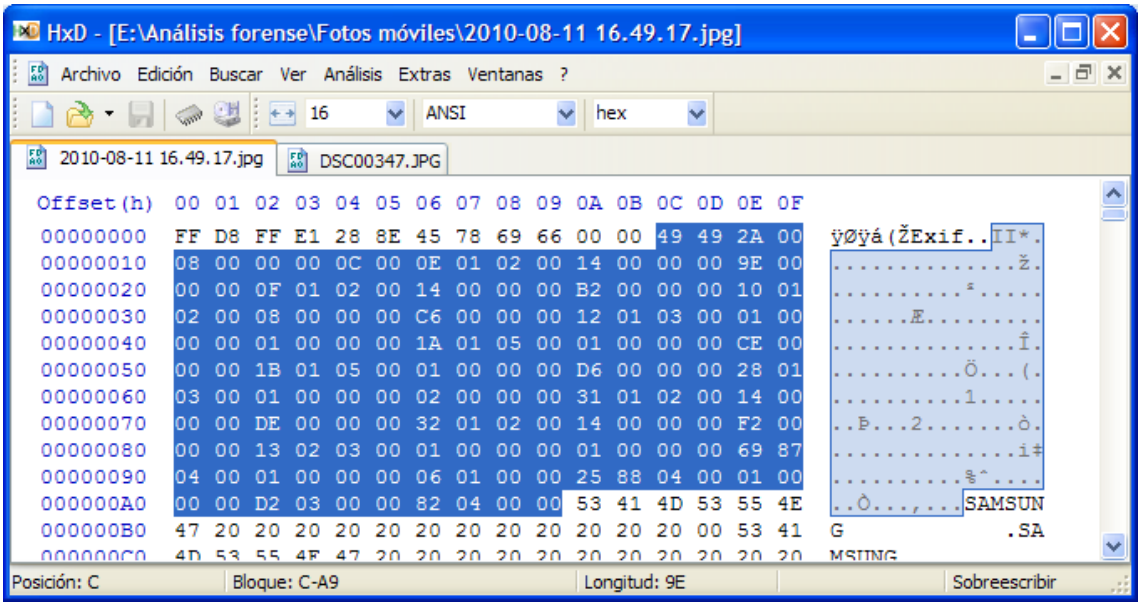


Fig. 13. Ejemplo del inicio de la etiqueta *Image Description* para Samsung Galaxy S

A partir de ese byte hay que contar 20 elementos de tipo ASCII (7-bit ASCII), por lo que los datos son los que se muestran en la figura 13 marcados en azul. Cabe destacar como se aprecia que los datos "SAMSUNG (12 espacios en blanco, '0x00')" terminan en NULL ('0x00'), siguiendo la especificación Exif (ver figura 14).

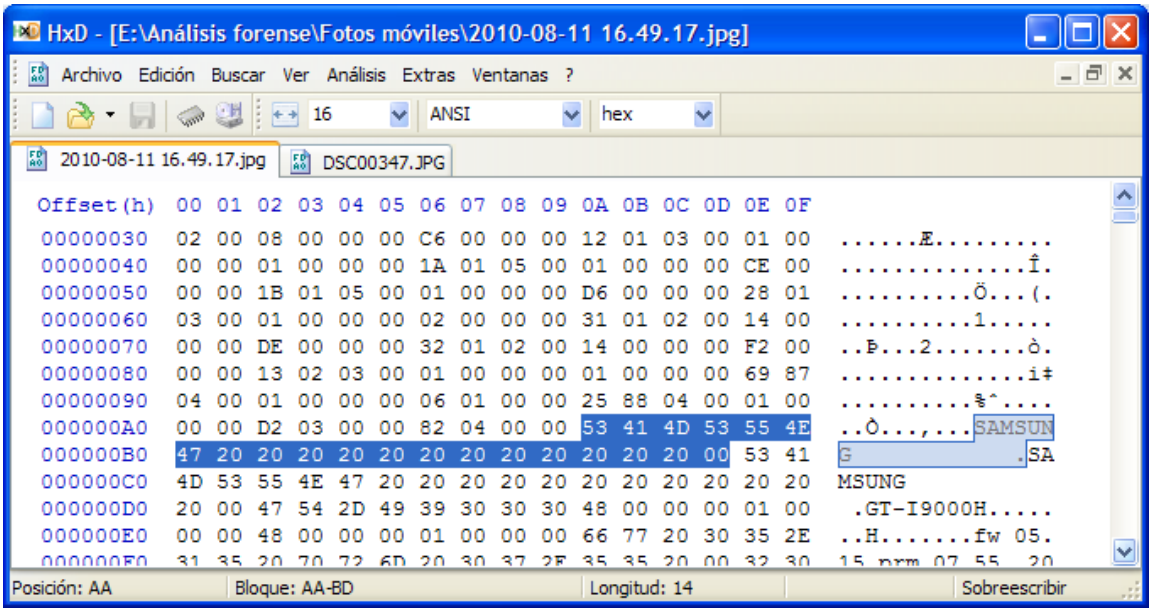


Fig. 14. Ejemplo de la estructura de la etiqueta *Image Description* para Samsung Galaxy S

Seguidamente se va a examinar el siguiente etiqueta del directorio "0th IFD" (IFD 0), para el mismo archivo. Teniendo en cuenta la información anterior, la etiqueta a examinar se muestra en la figura 15.

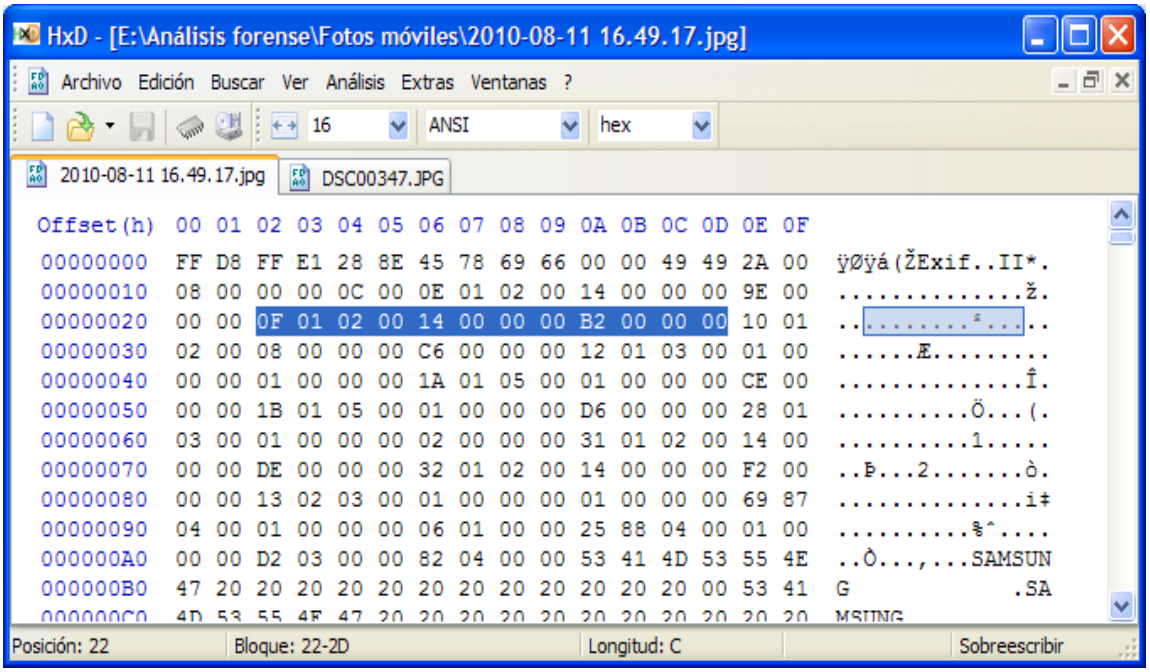


Fig. 15. Ejemplo de la segunda entrada del "0th IFD" para Samsung Galaxy S

La segunda entrada del directorio es la '0x0F01020014000000B2000000', cuyo significado es el siguiente:

- Etiqueta. ‘0x010F’. Etiqueta *Make*.
- Tipo. ‘0x0002’. ASCII.
- Nº de elementos. ‘0x00000014’, es decir, 20 elementos.
- Desplazamiento. ‘0x000000B2’ con respecto el inicio de la cabecera TIFF, es decir, 178 bytes.

Por tanto para obtener el valor de la etiqueta *Make* (ya que su tamaño es mayor de 4 bytes) tenemos que ir al lugar que nos indica el desplazamiento. En la mima figura se puede apreciar abajo que la longitud es ‘0xB2’ con respecto al inicio de la cabecera TIFF. Por lo que el inicio de los datos de la etiqueta es, por tanto, la posición ‘0xBE’ (ver figura 16).

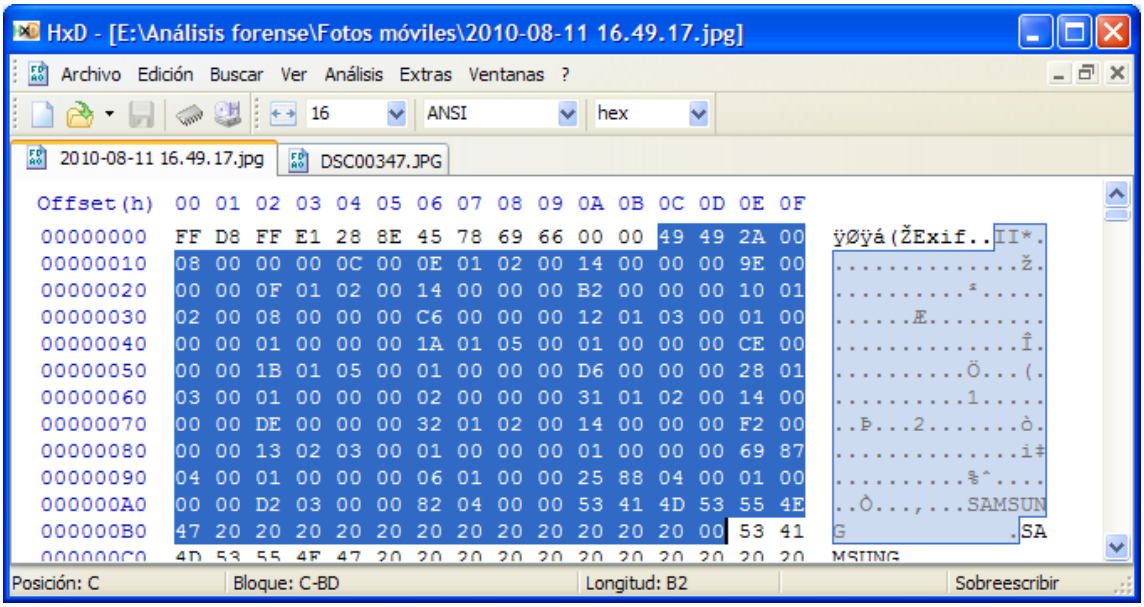


Fig. 16. Ejemplo del inicio de la etiqueta *Make* para Samsung Galaxy S

A partir de ese byte hay que contar 20 elementos de tipo ASCII (7-bit ASCII), por lo que los datos son los que se muestran en la figura 17 marcados en azul.

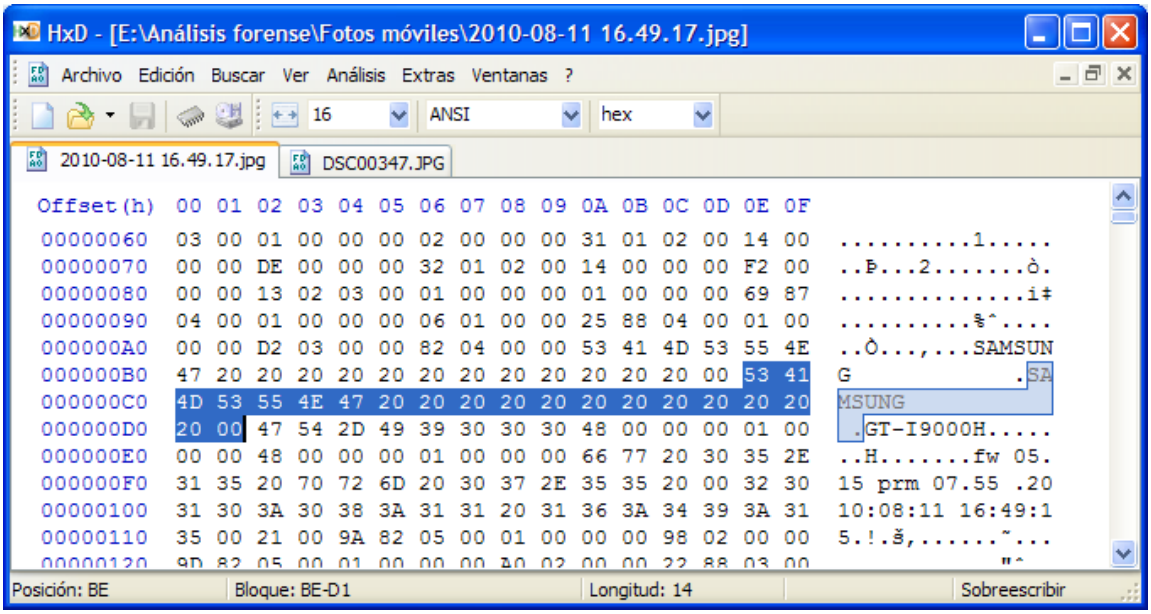


Fig. 17. Ejemplo de la estructura de la etiqueta *Make* para Samsung Galaxy S

Cabe destacar como se aprecia en el ejemplo que los datos "SAMSUNG (12 espacios en blanco – '0x00') terminan en NULL ('0x00')" siguiendo las especificación Exif. Asimismo se puede observar que dos etiquetas diferentes *Image Description* y *Make* para una misma imagen pueden tener los mismos valores, si bien su información debe ser duplicada para que se siga la especificación Exif.

A continuación se van a analizar los mismos elementos del IFD para la imagen del Sony Ericsson W580i. Tras la cabecera TIFF están los bytes '0x0A000F0102000E00000086000000'. Teniendo en cuenta siempre que la alineación es "Intel" ("II") los dos primeros bytes '0x0A00' indican cuantas entradas tiene el directorio actual, que es el directorio "0th IFD". Por tanto, el "0th IFD" tiene '0x000A' entradas, es decir 10 (ver figura 18).

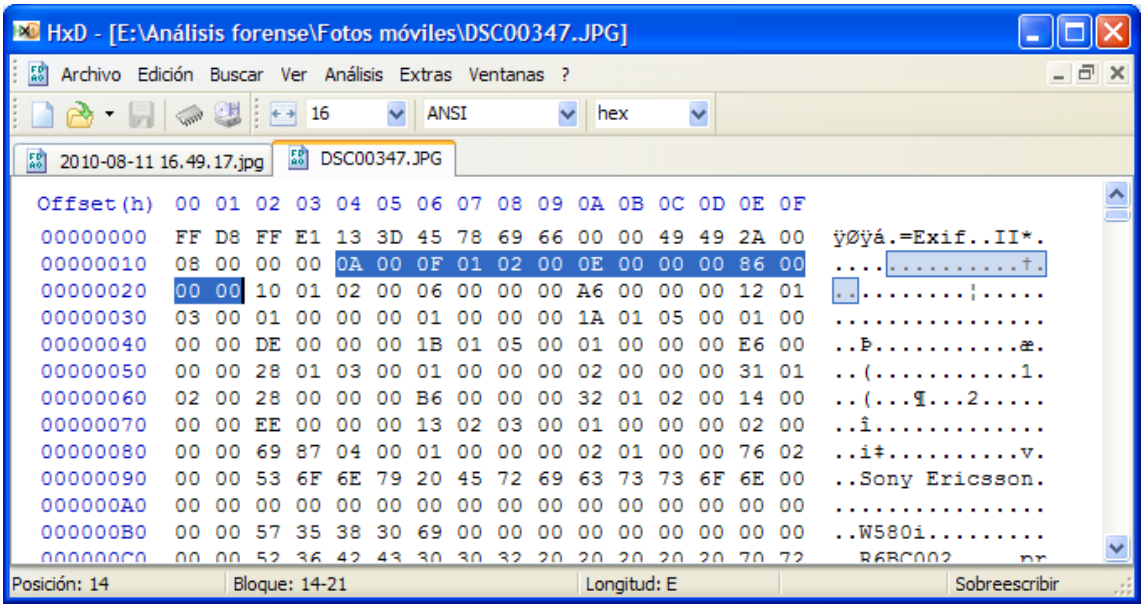


Fig. 18. Ejemplo de la primera entrada del "0th IFD" para Sony Ericsson W580i

En la imagen anterior se resaltan también en azul la primera entrada del directorio '0x0F0102000E00000086000000', que se interpreta de la siguiente forma:

- Etiqueta. '0x010F'. Etiqueta *Make*.
- Tipo. '0x0002'. ASCII.
- Número de elementos. '0x0000000E', es decir, 13 elementos.
- Desplazamiento. '0x00000086' con respecto el inicio de la cabecera TIFF, es decir, 134 bytes.

Por tanto para obtener el valor de la etiqueta *Make* (ya que su tamaño es mayor de 4 bytes) tenemos que ir al lugar que nos indica el desplazamiento. En la misma figura se puede apreciar abajo que la longitud es '0x86' con respecto al inicio de la cabecera TIFF. El inicio de los datos de la etiqueta comienza, por tanto, en la posición '0x92' (ver figura 19).

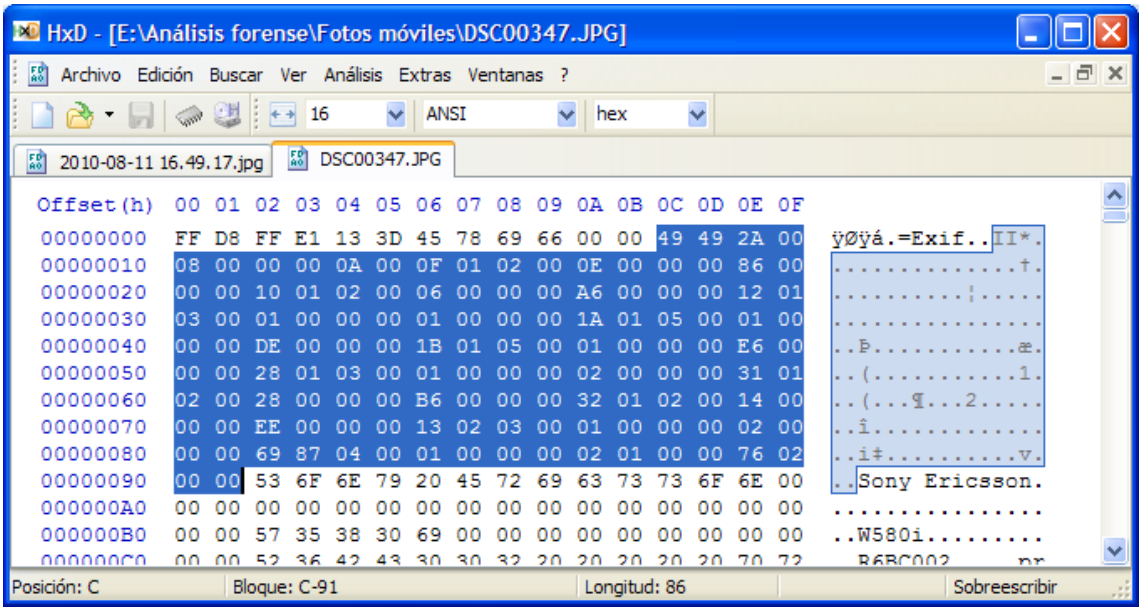


Fig. 19. Ejemplo del inicio de la etiqueta *Make* para Sony Ericsson W580i

A partir de ese byte hay que contar 13 elementos de tipo ASCII (7-bit ASCII), por lo que los datos son los que se muestran en la figura 20 marcados en azul.

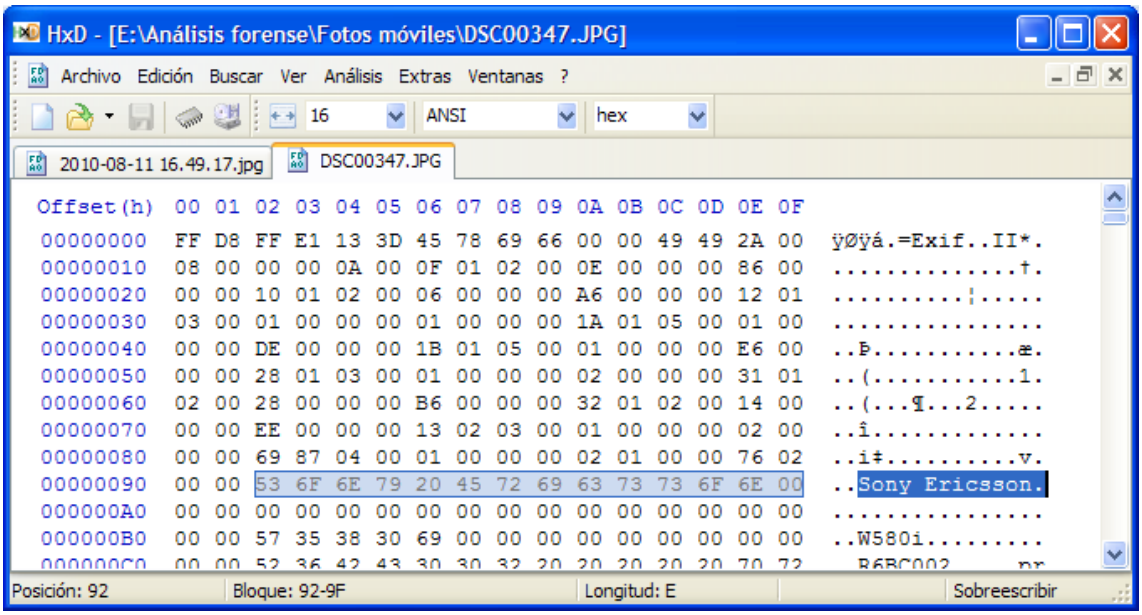


Fig. 20. Ejemplo de la estructura de la etiqueta *Make* para Sony Ericsson W580i

Cabe destacar como se aprecia en el ejemplo que los datos ("Sony Ericsson0x00") terminan en NULL ('0x00') siguiendo la especificación Exif.

Seguidamente vamos a examinar la siguiente etiqueta del directorio "0th

IFD" (IFD 0) para el mismo archivo. Teniendo en cuenta la información anterior, la segunda entrada del directorio es '0x10010200060000000A6000000', cuya interpretación se muestra en la figura 21.

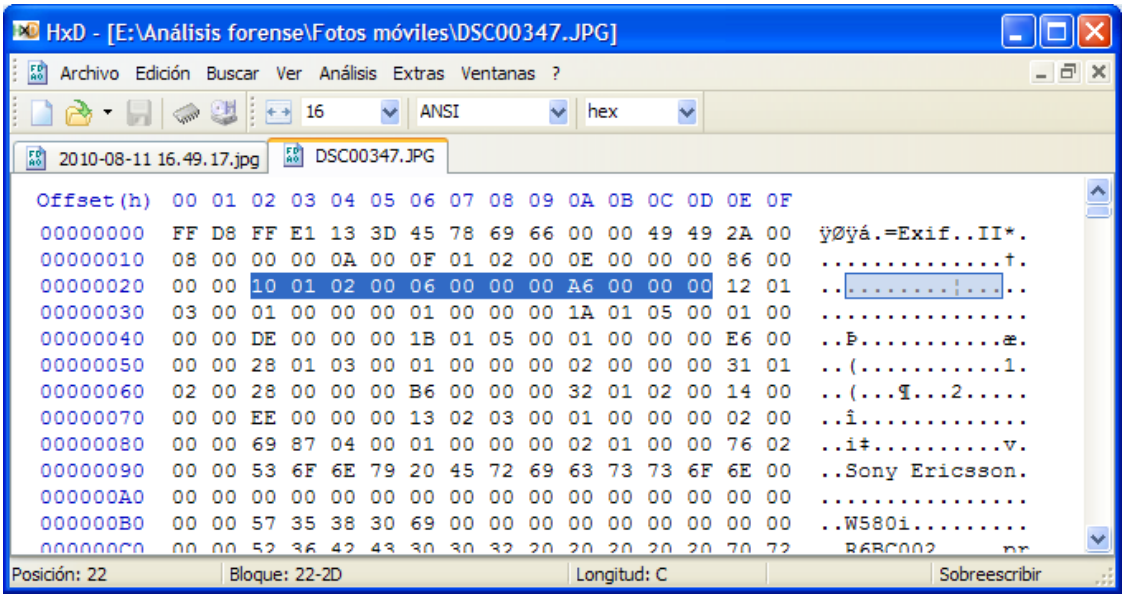


Fig. 21. Ejemplo de la segunda entrada del "0th IFD" para Sony Ericsson W580i

- Etiqueta. '0x0110'. Etiqueta *Model*.
- Tipo. '0x0002'. ASCII.
- Nº. de elementos. '0x00000006', es decir, 6 elementos.
- Desplazamiento. '0x000000A6' con respecto el inicio de la cabecera TIFF, es decir, 166 bytes.

Por tanto para obtener el valor de la etiqueta *Model* (ya que su tamaño es mayor de 4 bytes) tenemos que ir al lugar que nos indica el desplazamiento. En la misma figura se puede apreciar que la longitud es '0xA6' con respecto al inicio de la cabecera TIFF, El inicio de los datos de la etiqueta comienza, por tanto, en la posición '0xB2' (ver figura 22).

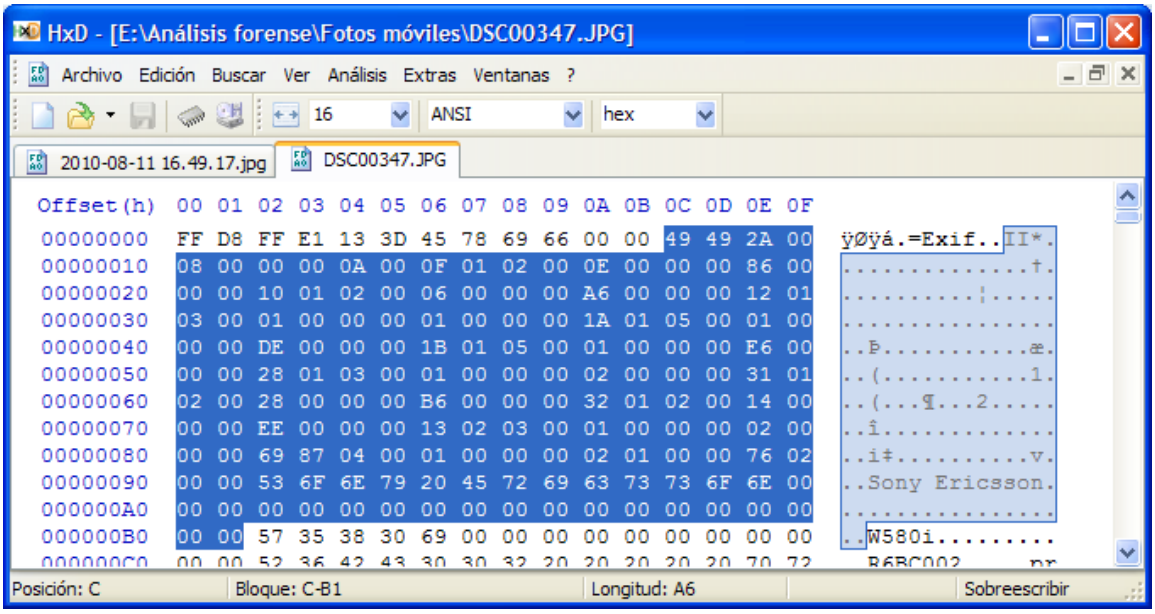


Fig. 22. Ejemplo del inicio de la etiqueta *Model* para Sony Ericsson W580i

A partir de ese byte hay que contar 6 elementos de tipo ASCII (7-bit ASCII), por lo que los datos son los que se muestran en la figura 23 marcados en azul. Cabe destacar que los datos ("W580i0x0000") terminan en NULL (0x00), siguiendo la especificación de Exif.

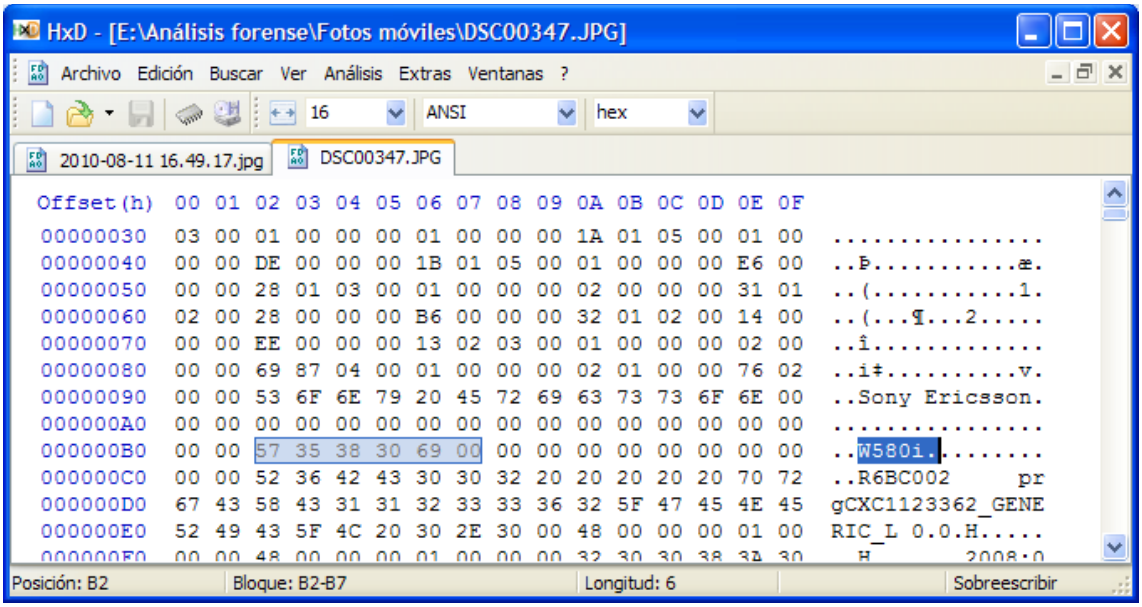


Fig. 23. Ejemplo de la estructura de la etiqueta *Model* para Sony Ericsson W580i

4.1. Anomalías en el seguimiento de la especificación Exif

Tras el análisis binario de varias imágenes se han detectado casos en los que no se sigue la especificación al 100%, aún indicando en su cabecera lo contrario. A continuación se mostrarán casos en los que el fabricante asegura que su imagen sigue Exif 2.2 y realmente no cumple la especificación.

En una imagen realizada con un Samsung Galaxy S se detecta que la entrada del directorio IFD0 es '0x1001020008000000C6000000', que se interpreta de la siguiente forma:

- Etiqueta. '0x0110'. Etiqueta *Model*.
- Tipo. '0x0002'. ASCII (según Exif 2.3 termina en NULL 0x00).
- Nº. elementos. '0x00000008', es decir, 8 elementos.
- Desplazamiento. '0x000000C6' con respecto el inicio de la cabecera TIFF, es decir, 198 bytes.

Por tanto como se observa ese desfase de '0xC6' desde el inicio de la cabecera TIFF apunta a la dirección '0xD2', donde se encuentra la información mostrada en la figura 24.

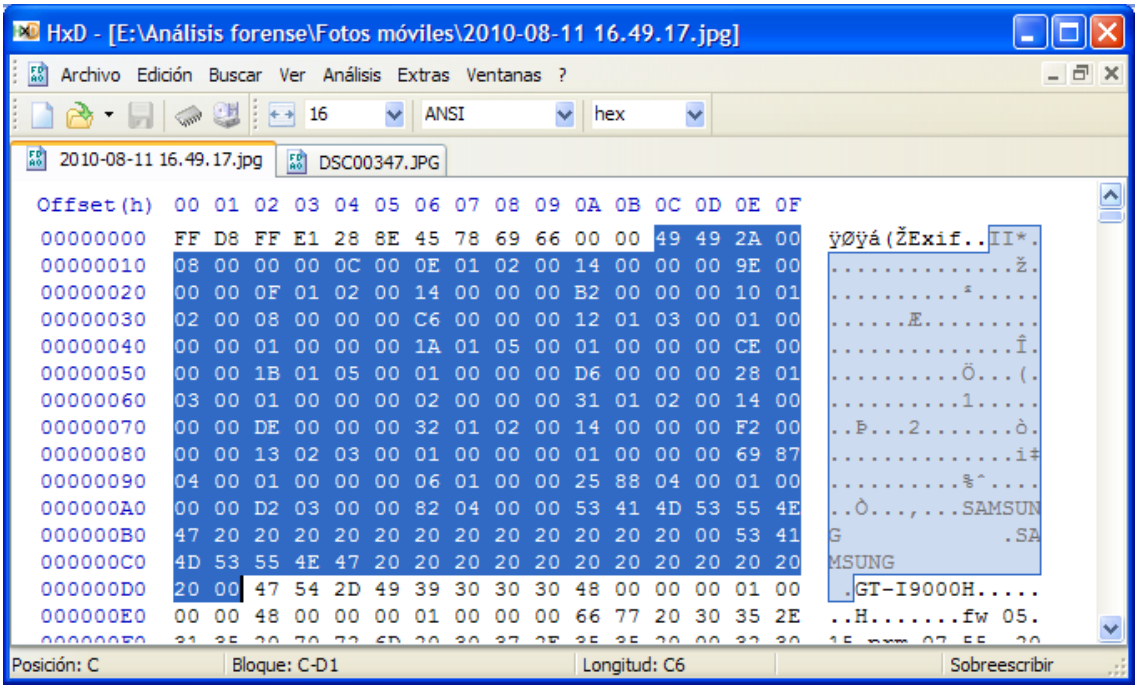


Fig. 24. Ejemplo del inicio de la etiqueta *Model* para Samsung Galaxy S

La información de la etiqueta *Model* es "GT-I9000" y tiene longitud 8 como se indicaba en la cabecera. A simple vista todo es correcto, pero siendo estrictos, esta imagen no cumple al 100% la especificación Exif 2.2, ya que se indica que el tipo es 2 (ASCII terminado en NULL – '0x00') y esta cadena no termina en NULL. Para almacenar "GT-I9000" se necesitan 9 elementos (8 caracteres ASCII + 1 NULL) y no 8 como indica la entrada del directorio (ver figura 25).

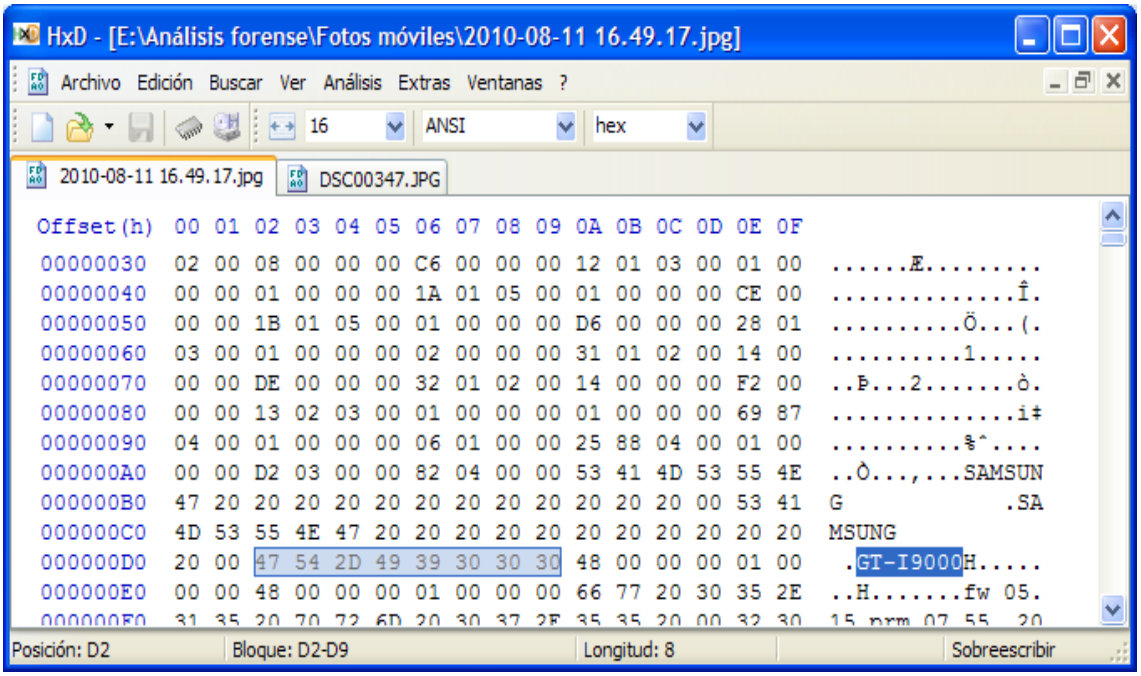


Fig. 25. Ejemplo de la estructura de la etiqueta *Model* anómalo para Samsung Galaxy S

Otro caso de este apartado es una imagen de un teléfono móvil Nokia N70, que asegura seguir la especificación Exif 2.2. Las etiquetas que se han analizado son las siguientes: '0xA004' (*Related Audio File*) y '0xA420' (*Unique Image ID*).

La primera etiqueta, *Related Audio File*, según la especificación es de tipo ASCII y posee 13 elementos. En la figura 26 se observa que la etiqueta en el archivo es: '0x04A0020001000000310052 02'.

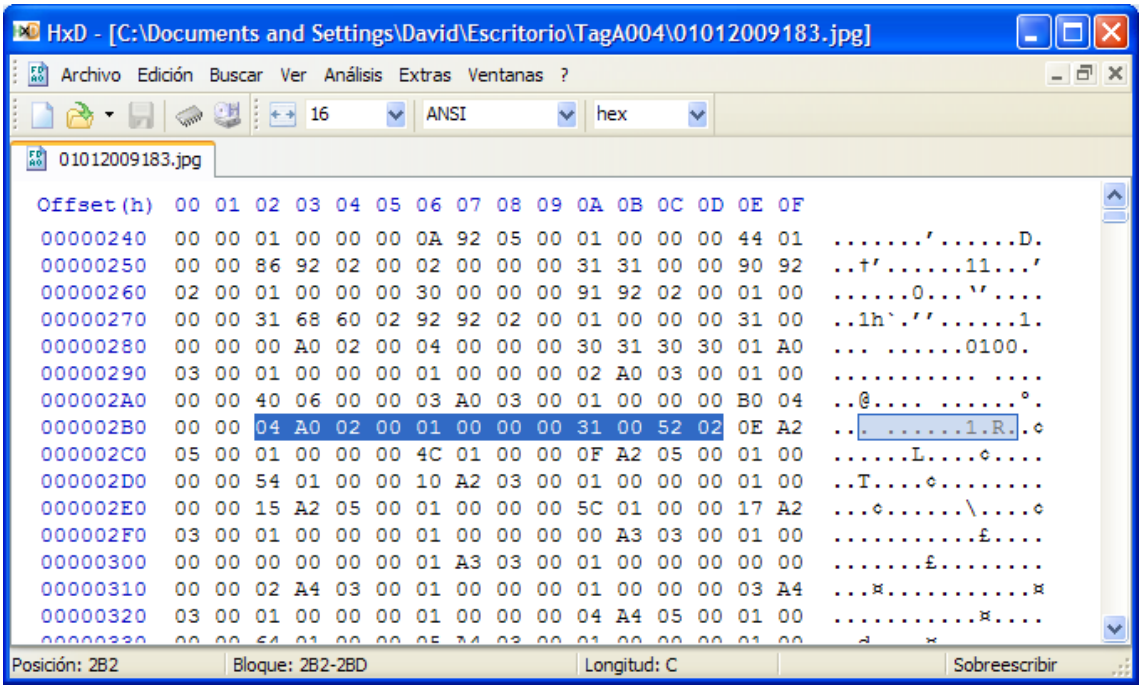


Fig. 26. Ejemplo de la estructura de la etiqueta *Related Audio File* anómalo para Nokia N70

Teniendo en cuenta que la alineación es "II" se puede observar que se almacena la etiqueta '0x04A0', seguido del tipo '0x0200', es decir, tipo ASCII, lo que según la especificación es totalmente correcto. A continuación viene el tamaño, que debería ser 13, es decir '0x0D000000' y realmente almacena '0x01000000', es decir 1, que viola claramente la especificación dos veces. En primer lugar porque la etiqueta *Related Audio File* indica que el tamaño de los datos tiene que ser 13 bytes y porque la especificación Exif indica que el tamaño mínimo de los datos tiene que ser 4 bytes.

Una vez visto que este archivo no sigue la especificación, los datos que se almacenan son '0x31005202'. Este valor es un 1 en ASCII, seguido del valor nulo '0x00', R en ASCII y el valor '0x02' (STX en ASCII). Este hecho puede generar problemas para los programas que extraen la información Exif por la incoherencia entre la especificación y los datos almacenados. Dado que este tipo de casos pueden llegar a ser numerosos, los visores de información Exif tienen que tomar un criterio uniforme para la extracción de cadenas ASCII. Las distintas opciones posibles son:

1. En casos de violación de la especificación no mostrar los datos e indicar un error en el análisis sintáctico ya que no se sigue la misma. Esta opción es la más restrictiva y purista, ya que no permite ningún tipo de "licencias" sobre la especificación. Las siguientes opciones muestran alternativas que permiten la extracción de la información de la imagen a costa de pasar por alto el seguimiento estricto de la especificación Exif.

2. Tomar la consideración de extraer todos los datos del tipo ASCII hasta que se encuentre el primer nulo ('0x00'). Esta opción puede hacer que se generen errores graves, ya que si las cadenas ASCII no terminan en nulo, se pueden mostrar datos no pertenecientes a la etiqueta en el peor de los casos puede producir desbordamientos de memoria si en los bytes sucesivos a la etiqueta no existiera el valor nulo.

3. Extraer todos los datos teniendo únicamente en cuenta el tamaño indicado de los mismos. Esta es la opción menos restrictiva, ya que mostraría los caracteres ASCII del tamaño indicado, aunque éstos no cumplieran las restricciones de la especificación Exif.

4. Opción mixta entre la 2 y la 3. Es decir extraer todos los datos teniendo el cuenta el tamaño de los mismo y separando las distintas cadenas teniendo en cuenta el nulo ('0x00') como separador.

Con respecto a los casos expuestos anteriormente, el visor *Exif Viewer* muestra exactamente "1;R{{STX}}", lo cual indica que toma como opción la 4. Separa con punto y coma las dos subcadenas ASCII, ya que hay una terminación de la primera con nulo ('0x00') y sigue mostrando los datos hasta el tamaño de los datos.

Teniendo en cuenta que el tamaño mínimo de los datos de una etiqueta es 4 bytes (ya que si es menor se tienen que "ocupar" los cuatro bytes destinados al campo datos de la etiqueta) la forma de presentar los datos de *PhotoInfoEx*

parece ser el mostrar estrictamente el número de elementos que dicta la etiqueta, es decir, la opción 3, no visualizando posible información sin inicializar o "basura".

Independientemente de la forma de mostrar los datos de los dos visores Exif, hay un problema en la creación del archivo por parte del fabricante al no seguir fielmente la especificación.

Otro caso se da en el mismo teléfono móvil (Nokia N70) y en la etiqueta *Unique Image ID*. La especificación indica que es de tipo ASCII y con 33 elementos. En la figura 27 se observa que la etiqueta en el archivo es: '0x20A402000100000031909504'.

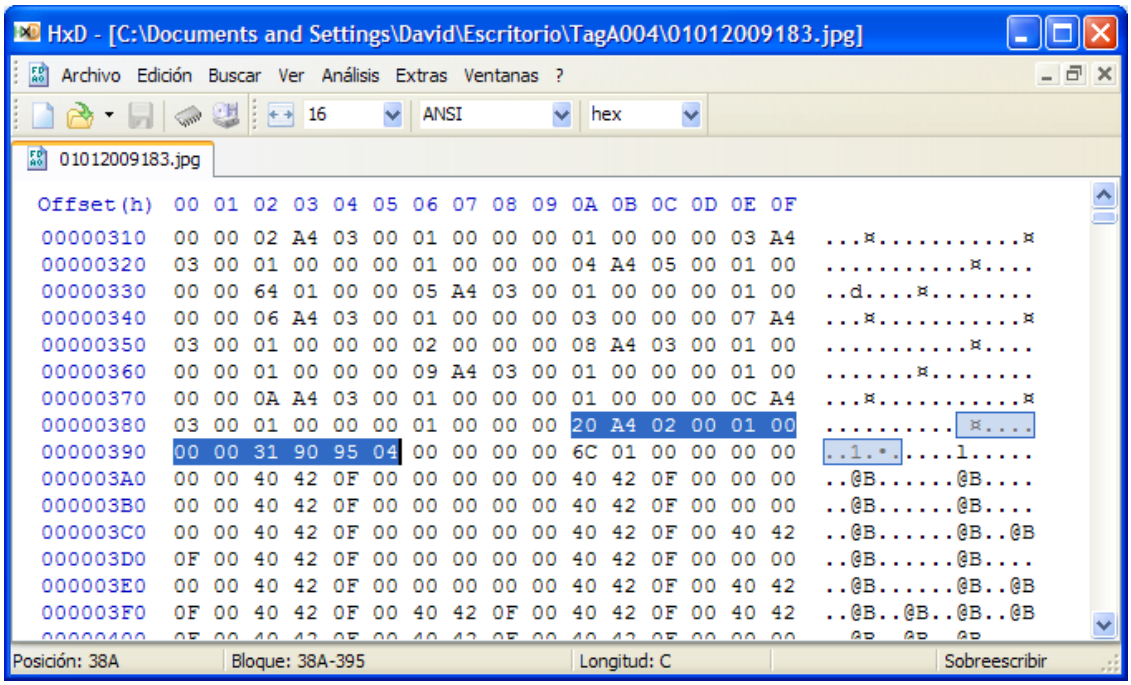


Fig. 27. Ejemplo de la estructura de la etiqueta *Unique Image ID* anómalo para Nokia N70

Teniendo en cuenta que la alineación es "II" se puede observar que se almacena la etiqueta '0xA420', seguido del tipo '0x0002', es decir, tipo ASCII, que según la especificación es totalmente correcto. Tras estos datos viene el tamaño, que debería ser 33, es decir, '0x21000000' y realmente almacena '0x01000000', es decir, 1, que viola claramente la especificación, como en el caso

anterior por partida doble. Una vez visto que este archivo no sigue la especificación, los datos que se guardan son '0x31909504', teniendo en cuenta 4 bytes, ya que el análisis revela que el quinto byte es el comiendo de otro nueva etiqueta. Este hecho hace que se viole de nuevo la especificación, ya que en el tipo ASCII es obligatorio que termine en nulo (0x00) y en este caso el nulo no aparece en la cadena. Asimismo, existe otra violación de la especificación ya que los caracteres ASCII son de 7 bits (rango de 0-127, '0x00'-'0x7F'), por lo que los caracteres '0x90' y '0x95' están totalmente fuera de lo que permite la especificación.

El visor *PhotoInfoEx* muestra un 1, por lo que no muestra los datos hasta el primer nulo, observando que en este caso se sigue también la opción de análisis sintáctico número 3. Para poder asegurar en qué caso de los anteriormente expuestos con respecto a la muestra de datos ASCII se encuentra *PhotoInfoEx*, se va a modificar el archivo indicando que para la etiqueta '0x04A0' examinado, el tamaño de los datos es 3 (lo que sigue violando la especificación) y que los datos son '0x31004848', por lo que la etiqueta completa quedaría como '0x20A4020003000000031004848'. Tras este cambio se observa en *PhotoInfoEx* que los datos mostrados son "1 H", con lo que se puede asegurar que muestra los datos según la opción 3 (teniendo en cuenta únicamente la longitud de los datos).

Asimismo, se observa que al hacer "clic" en los datos para editarlos, el valor pasa a ser "1" y simplemente realizar esta acción y no hacer ninguna otra más hace que el programa tome ese campo como editado. Al cambiar de foto nos indica si queremos guardar los cambios, por lo que prueba que la edición de datos ASCII por *PhotoInfoEx* (aunque no la visualización) sigue la especificación estrictamente, no permitiendo insertar cadenas que no terminen en nulo. En la aplicación que hemos desarrollado decidimos tomar este mismo criterio, ya que el seleccionar el criterio más "purista" (opción 1) puede ser perjudicial para la tarea del análisis forense.

Para el caso de la etiqueta *Image Unique ID* ('0xA420'), sin ningún tipo de modificación, *Exif Viewer* muestra "1•{{EOT}}" (dos blancos entre 1 y EOT), es decir cuatro caracteres mostrando los que pertenecen al rango válido de la especificación Exif y un blanco cuando no pertenecen a un rango válido. Una vez realizado el cambio en el archivo descrito anteriormente, es decir, cambiar los datos de la etiqueta '0x04A0', *Exif Viewer* muestra los datos como "1;HH", por lo que se puede corroborar que muestra los datos de la forma indicada en el caso 4, separando las distintas cadenas con ";" (separador nulo '0x00'). Aún así para todos estos casos, es conveniente reseñar que el problema proviene del fabricante que no sigue la especificación Exif.

En este apartado se han mostrado algunos ejemplos de las anomalías detectadas tras el análisis binario manual de las imágenes, pero no han sido las únicas ya que se han encontrado más en otras imágenes y otras etiquetas como *Exif version*, *Meetering Mode*, *Exposure Program*, *DateTimeOriginal*, etc., Por tanto, se puede concluir que muchos de los fabricantes no siguen fielmente las especificaciones Exif, indicando en el propio archivo lo contrario, lo que puede producir graves problemas en la extracción de los metadatos de las imágenes por medio de aplicaciones, así como problemas de interoperabilidad entre distintos dispositivos.

5. HERRAMIENTA PARA EL ANÁLISIS FORENSE DE IMÁGENES DE DISPOSITIVOS MÓVILES

Una vez vistos ejemplos del análisis binario manual de los metadatos Exif en imágenes, claramente se puede observar que la obtención de los metadatos a ese nivel es tediosa y lenta. Por tanto, se necesitan herramientas para la extracción automática y su visualización de forma gráfica. Este tipo de herramientas sirven de apoyo a la tarea del analista forense en lo que respecta al análisis de los metadatos. Sin el uso de este tipo de aplicaciones sería complejo realizar el procesamiento para un gran número de imágenes.

En este trabajo se ha desarrollado una herramienta que facilita la extracción y el tratamiento de metadatos Exif en imágenes JPEG. A grandes rasgos la herramienta se divide en dos grandes partes:

- **Tratamiento de imágenes a nivel individual.** Este parte permite obtener la información Exif detallada de una imagen individual, así como situarla geográficamente en Google Maps y Google Earth (si posee información de geoposicionamiento). A la hora de mostrar la información Exif se ha organizado en 6 grupos: *Image*, *Exif*, *GPS*, *Interoperability*, *Thumbnail* y *Maker Note*.

- **Tratamiento de imágenes a nivel de grupo.** En este bloque se permiten realizar consultas avanzadas sobre los metadatos Exif de distintos proyectos o conjuntos de imágenes. Asimismo, existe la opción de situar las imágenes que posean información de geoposicionamiento en Google Maps.

En el anexo A se muestra el funcionamiento de la herramienta desarrollada.

5.1. Comparativa con otras herramientas

Para realizar una comparativa de la herramienta desarrollada con otras con fines similares, se han buscado principalmente herramientas de extracción y tratamiento de metadatos Exif para archivos JPEG, aunque no ha sido un criterio que excluya a otro tipo de herramientas relacionadas.

En la evaluación se han tenido en cuenta diversos aspectos, aunque se ha dado mayor importancia a los relacionados con la extracción y el tratamiento de los metadatos Exif. Se realizará una comparativa con las aplicaciones *PhotoInfoEx*, *JHead*, *ExifTool*, *Exif Viewer* y *ExifPro Image Viewer*.

5.1.1. PhotoInfoEx

PhotoInfoEx es un programa de fotografía digital que permite editar o modificar ciertos metadatos de la información Exif o IPTC de los archivos de imágenes en formato JPEG y TIFF, así algunos archivos tipo de RAW. Es una aplicación propietaria para sistemas operativos Windows [16].

Las principales ventajas sobre la herramienta desarrollada son la mejor navegación sobre los archivos a examinar, la exportación de los metadatos obtenidos a Microsoft Excel y Microsoft Word y la impresión de los mismos.

Como inconvenientes con respecto a la herramienta desarrollada se destacan:

- Problemas en la extracción de metadatos Exif que no son acordes al 100% con la especificación. Por ejemplo se han detectado imágenes con datos en la etiqueta *DateTimeOriginal* errónea para la fecha. *PhotoInfoEx* en lugar de mostrar un error o la cadena tal como está almacenada, formatea los datos internamente y muestra otros distintos a los que posee la imagen, aparentemente correctos cuando realmente no lo son.

- No permite ningún tipo de análisis grupal de fotos. Este es el principal inconveniente que engloba un gran número de problemas con respecto al

análisis forense de los metadatos en imágenes. No se permite el tratamiento de imágenes en proyectos independientes, y como consecuencia no se posibilitan las consultas en conjunto (*Query Set*), consultas avanzadas (*Advanced Query*) y el tratamiento de geoposicionamiento de conjuntos de imágenes. Esta carencia es de elevada importancia, ya que es uno de los puntos fuertes que la experiencia ha señalado de la herramienta desarrollada.

El segundo inconveniente citado es clave y, por tanto, la valoración final es que, aunque siendo conscientes de pequeños aspectos ventajosos por parte de *PhotoInfoEx* en la navegación de los archivos, la herramienta desarrollada es muchísimo más potente, útil y versátil para el objetivo para el que fue enfocada.

5.1.2. JHead

JHead es una herramienta de línea de comandos que permite extraer y manipular la información Exif de los archivos JPEG. Es una aplicación de software libre para sistemas operativos Windows, GNU/Linux y Mac Os-X [40].

La única ventaja destacable de *JHead* frente a la aplicación desarrollada es que permite la extracción de los metadatos IPTC y XMP (aunque éstos no sean utilizados por los dispositivos móviles).

El principal inconveniente es que, al igual que PhotoInfoEx, no permite el análisis grupal de fotos, lo cual es fundamental. Carece de interfaz gráfica por lo que hace la tarea del analista forense más pesada y tediosa. Además no posee funciones de geoposicionamiento en Google Maps y Google Earth.

Por tanto, se concluye que es una herramienta con muchas menos posibilidades y más difícil de utilizar que la herramienta desarrollada.

5.1.3. ExifTool

ExifTool es una aplicación que permite la extracción y edición de metadatos en una gran variedad de formatos de archivos [41]. Soporta formatos de metadatos tales como Exif, IPTC, XMP, JFIF. Además, permite decodificar información propia de los fabricantes (*maker note info*) de gran cantidad de cámaras digitales de marcas como Canon, Casio, FujiFilm, HP, Kodak, Nikon, Panasonic, Ricoh, Samsung y Sony, entre otras. Es una aplicación de software libre para sistemas operativos Windows, GNU/Linux y Mac Os-X.

Básicamente las ventajas e inconvenientes de *ExifTool* con respecto a la herramienta desarrollada son los mismos que con *JHead* y, consecuentemente,las conclusiones de la comparación.

5.1.4. Exif Viewer

Exif Viewer es un complemento para el navegador Firefox que permite extraer metadatos Exif, IPTC y XMP, de imágenes JPEG tanto locales como remotas. Es una aplicación de software libre [42].

La principal ventaja de *Exif Viewer* con respecto a la aplicación desarrollada es su facilidad y rapidez en la instalación, así como la facilidad de uso (teniendo en cuenta las grandes limitaciones que tiene). Otra de las ventajas es que permite el geoposicionamiento además de, en Google Maps y Google Earth, en Yahoo! Maps y en MSN Maps & Directions.

El principal inconveniente, al igual que con todas las herramientas anteriormente comparadas, es que no permite un análisis de las imágenes en grupo, que insistimos es clave. Asimismo, la forma de presentar la información y el interfaz es austero y poco amigable.

5.1.5. ExifPro Image Viewer

ExifPro Image Viewer es una aplicación que permite mostrar la información Exif (un número muy limitado de etiquetas) de imágenes JPEG. Es una aplicación propietaria para sistemas operativos Windows [43].

La principal ventaja de esta aplicación sobre todas las anteriormente tratadas (incluida la que se ha desarrollado) es el navegador de archivos de las imágenes. Ofrece una cantidad inmensa de posibilidades para mostrar, agrupar y ordenar las imágenes de los directorios. Sin duda, en este aspecto es la más poderosa. Asimismo, es la más potente con respecto a la forma de mostrar las imágenes individuales, ya que posee muchas opciones para su visualización (rotación, cambio de tamaño, etc).

Con respecto a la extracción y tratamiento de los metadatos, sin duda, es el que más carencias tiene. Es una aplicación que apenas extrae una veintena de etiquetas Exif que presenta de una forma poco clara. No posee ningún tipo de funcionalidad de geoposicionamiento. Además, no permite el tratamiento grupal de los metadatos de las imágenes.

Posee una opción que posibilita la exportación de la información Exif incluida en fotografías JPEG a un fichero TXT, pudiendo configurar un carácter separador entre las distintas etiquetas extraídas. Esto facilita la posterior importación de la información del archivo TXT a otros formatos de bases de datos u hojas de cálculo. Posteriormente a esto, se pueden realizar consultas grupales sobre los datos exportados, pero la aplicación no permite directamente este tipo de operación, además de requerir al analista forense de conocimientos informáticos avanzados para realizar este tipo de tratamiento.

Por tanto las conclusiones que se obtienen de la comparativa es que esta herramienta más que ser una herramienta para el tratamiento de metadatos Exif, es una herramienta para la visualización y clasificación de imágenes. El

conjunto de datos Exif que obtiene es excesivamente limitado y en ninguna circunstancia es una aplicación válida para la tarea de análisis forense.

5.1.6. Conclusiones de la comparativa

Una vez comparada la herramienta una a una con otras con propósitos comunes, se puede concluir que, no habiendo ninguna que ofrezca todas las mejores posibilidades, sin duda la herramienta presentada en este trabajo es la que ofrece una mayor funcionalidad y versatilidad en el tratamiento de metadatos Exif. En la tabla 8 se muestra una tabla comparativa de todas las herramientas evaluadas.

Ninguna de las aplicaciones comparadas posee un tratamiento de imágenes en grupo, así como una extracción de metadatos Exif más completa y organizada. Esta aplicación no tiene como objetivo primordial la visualización de galerías de imágenes, sino favorecer y automatizar, en la medida de lo posible, la tarea del análisis forense de imágenes de dispositivos móviles con respecto a los metadatos. Este objetivo se consigue con mayor éxito que con cualquiera de las herramientas presentadas en la comparación.

	Plataforma	Interfaz	Versión EXIF	Visualización de los Datos EXIF	Edición Información EXIF	Formatos de metadatos	Software libre	Observaciones
Aplicación desarrollada	– Windows – GNU/Linux	Gráfica	2.3	Organizada por IFD	No	Exif	Sí	– Interfaz intuitiva y amigable. – Análisis en grupo.
PhotoInfoEx	– Windows	Gráfica	2.21	Organizada por IFD	Sí	Exif, IPTC	No	– Exportación de metadatos a otros formatos.
Jhead	– Windows – Mac Os-X – GNU/Linux	Comandos	No especificada	No organizada	Parcial	Exif, IPTC, XMP	Sí	– Difícil uso. – Funcionalidades GPS reducidas.
ExifTool	– Windows – Mac OS X – GNU/Linux	Comandos	No especificada	No organizada	Sí	Exif, IPTC, XMP, JFIF	Sí	– Difícil uso. – Funcionalidades GPS reducidas.
Exif Viewer	– Complemento de Firefox	Gráfica	No especificada	Organizada por IFD	No	Exif, IPTC, XMP	Sí	– Metadatos de imágenes remotas.
ExifPro Image Viewer	– Windows	Gráfica	No especificada	No organizada	No	Exif	No	– Etiquetas de información Exif limitados. – Sin funcionalidad GPS.

Tabla 8. Tabla comparativa entre aplicaciones existentes

6. ANÁLISIS DE UN BANCO DE IMÁGENES MEDIANTE LA HERRAMIENTA

Una vez realizada una comparativa de la herramienta desarrollada con otras aplicaciones con fines análogos, en este apartado se va a realizar un análisis de un conjunto de imágenes reales de dispositivos móviles utilizando las distintas funcionalidades de la herramienta desarrollada.

El objetivo del análisis es la búsqueda da datos de interés, patrones de valores o simplemente información estadística sobre los metadatos Exif del banco de imágenes.

Las imágenes han sido obtenidas de dispositivos móviles de personas conocidas, que además de aportar los archivos, han aportado la información sobre la marca y modelo del dispositivo. Se ha intentado buscar la máxima heterogeneidad posible con respecto a las marcas y los modelos de los dispositivos, así como contar con el mayor número de imágenes de cada uno de ellos. El banco de imágenes está formado por 1840 imágenes de 9 marcas y 50 modelos. En la tabla 9 se muestran los modelos agrupados por marca con sus correspondiente número de imágenes.

Marca	Modelos	Número de Fotos
Research In Motion	BlackBerry 8100	3
	BlackBerry 8350i	1
	BlackBerry 8520	183
	BlackBerry 8900	3
	BlackBerry Bold 9000	24
	BlackBerry Curve 8320	3
HTC	HTC Hero	5
	HTC Tynii	31
	HTC Desire HD	133
Apple	IPhone	15
	IPhone 3G	33
	IPhone 3GS	38
	IPhone 4G	4
LG	LG KU990i	144
Motorola	Motorola W377	20
Nokia	Nokia 2630	7
	Nokia 5230	19
	Nokia 5300	100
	Nokia 5530	14
	Nokia 5800	28
	Nokia 6020	30
	Nokia 6085	4
	Nokia 6110	35
	Nokia 6120	20
	Nokia 6210 Navigator	24
	Nokia 6230i	21
	Nokia 6300	154
	Nokia 6303 Classic	35
	Nokia 6601	36
	Nokia E661	36
	Nokia E72-2	1
	Nokia N70	13
	Nokia N95	131
	Nokia N97	4
Samsung	Samsung Caliber SCH-R860	2
	Samsung Galaxy S	15
	Samsung H1	6
	Samsung Restore SPH-M570	1
	Samsung SGH-F250L	4
	Samsung SGH-F480	1
Sony Ericsson	Sony Ericsson C702	58
	Sony Ericsson K550	4
	Sony Ericsson Satio	26
	Sony Ericsson T707	102
	Sony Ericsson W205	1
	Sony Ericsson W580i	158
	Sony Ericsson W705	19
	Sony Ericsson W910i	20
	Sony Ericsson X10 Mini	10

Tabla 9. Teléfonos móviles clasificados por marca y modelo

A diferencia de los estudios realizados en las referencias citadas en puntos anteriores, el número de modelos de cámaras que se ha utilizado en los análisis posteriores es mucho mayor.

6.1. Análisis de la información de marca y modelo

Uno de los principales objetivos de la herramienta es la identificación de la fuente de la imagen, de ahí que se comience por este estudio. Primeramente se va a utilizar *Query Set* para obtener cuantas imágenes hay de cada marca y modelo. Estos datos han de compararse con la tabla 9 y de forma estadística (siempre sobre nuestro banco de imágenes), se podrá valorar el porcentaje de seguimiento que los fabricantes hacen sobre la inserción de estos dos metadatos. Los resultados de este análisis se muestran en la tabla 10.

Marca	Modelos	Número de Fotos	Número de Fotos Datos Exif	Porcentaje de Seguimiento
Research In Motion	BlackBerry 8100	3	3	100%
	BlackBerry 8350i	1	1	100%
	BlackBerry 8520	183	183	100%
	BlackBerry 8900	3	3	100%
	BlackBerry Bold 9000	24	24	100%
	BlackBerry Curve 8320	3	3	100%
HTC	HTC Hero	5	5	100%
	HTC Tynii	31	31	100%
	HTC Desire HD	133	133	100%
Apple	IPhone	15	19 *	-
	IPhone 3G	33	33	100%
	IPhone 3GS	38	38	100%
	IPhone 4G	4	0 *	-
LG	LG KU990i	144	144	100%
Motorola	Motorola W377	20	20	100%
Nokia	Nokia 2630	7	0	0%
	Nokia 5230	19	19	100%
	Nokia 5300	100	100	100%
	Nokia 5530	14	14	100%
	Nokia 5800	28	28	100%
	Nokia 6020	30	0	0%
	Nokia 6085	4	4 **	100%
	Nokia 6110	35	35	100%
	Nokia 6120	20	20	100%
	Nokia 6210 Navigator	24	24	100%
	Nokia 6230i	21	0	0%
	Nokia 6300	154	154	100%
	Nokia 6303 Classic	35	35	100%
	Nokia 6601	36	36	100%
	Nokia E661	36	36	100%
	Nokia E72-2	1	1	100%
	Nokia N70	13	13	100%
	Nokia N95	131	131 ***	100%
	Nokia N97	4	4	100%
Samsung	Samsung Caliber SCH-R860	2	2	100%
	Samsung Galaxy S	15	15	100%
	Samsung H1	6	6	100%
	Samsung Restore SPH-M570	1	1	100%
	Samsung SGH-F250L	4	4	100%
	Samsung SGH-F480	1	1	100%
Sony Ericsson	Sony Ericsson C702	58	58	100%
	Sony Ericsson K550	4	4	100%
	Sony Ericsson Satio U1a	26	26	100%
	Sony Ericsson T707	102	102	100%
	Sony Ericsson W205	1	1	100%
	Sony Ericsson W580i	158	158	100%
	Sony Ericsson W705	19	19	100%
	Sony Ericsson W910i	20	20	100%
	Sony Ericsson X10 Mini	10	10	100%
Sin identificar		-	58	-

Tabla 10. Resultados del análisis de la información de marca y modelo

* Las imágenes del IPhone 4 tienen como valor de modelo "IPhone", con lo cual las hace indistinguibles con respecto a las realizadas con el IPhone (modelo diferente a IPhone 4).

** En modelo se almacena el valor "Nokia 0001".

***En modelo se almacenan 66 imágenes con el valor "N95" y 65 con el valor "N95 8GB", dado que son dos versiones del mismo modelo.

La primera conclusión de este análisis es positiva, ya que se puede apreciar un alto grado de seguimiento por parte de los fabricantes a la hora de almacenar correctamente los valores para marca y modelo. Salvo "Nokia" todos los modelos evaluados tienen valores en marca y modelo (aunque en algunos casos descritos anteriormente no son completamente correctos).

Otro aspecto destacado de este análisis es la escasa uniformidad de los propios fabricantes a la hora de añadir la información de marca y modelo en las etiquetas Exif. Es decir no utilizan siempre la misma cadena para la marca o incluso puede haber una misma cadena para distintos modelos (caso IPhone y IPhone4), lo cual puede dar pie a graves errores en la identificación. Por ejemplo Sony Ericsson utiliza dependiendo del modelo la cadena "SEMC", "Sony Ericcson" o "SONY ERICCSON" para almacenar la marca, o "Research In Motion" utiliza indistintamente en los modelos de "BlackBerry" la cadena "RIM" o "Reserach In Motion" para el mismo fin.

Asimismo, utilizaremos *Advanced Query* para identificar cuáles son concretamente las imágenes que no contienen la información de marca y modelo. En el resultado se obtienen las imágenes concretas y son todas las de los modelos "Nokia 2630", "Nokia 6020" y "Nokia 6230".

6.2. Análisis de la información de las etiquetas *Image* y *Exif*

En este apartado se analizan las etiquetas Exif que se encuadran en los bloques *Image Info* y *Exif Info*. Primeramente con *Query Set* se examinarán cuales son las imágenes que no poseen información en ninguno de estos dos estos dos bloques. El resultado de este análisis es que todas la imágenes poseen información *Image Info* y *Exif Info* salvo las 58 sin marca y modelo.

Además en el bloque *Image Info* se analizará con *Query Set* el campo *Software Used*. Este campo puede ser de importancia para el análisis forense, ya que puede aportar datos de como es el proceso software de creación de la imagen. Los resultados obtenidos revelan uniformidad en el nombrado de versiones por parte de cada fabricante. Entre los distintos fabricantes la discordancia es total. También se destaca que el software utilizado parece variar en función de la operadora del móvil para un mismo modelo. Por ejemplo para un Sony Ericcson W580i la etiqueta *Software Used* tiene valores del estilo "R8BE001 prgCXC1123474_ORANGE_LA 0.0" (para operadora Orange) y "R8BE001 prgCXC1123362_GENERIC_L 0.0" (para cualquier operadora).

6.3. Análisis de la información *GPS*

En este apartado se analizan las etiquetas Exif que se encuadran en el bloque *GPS Info*. Primeramente con *Query Set* se examinarán cuales son las imágenes que no poseen información en este bloque. Este análisis es muy subjetivo, ya que depende de si el terminal tiene GPS integrado, que el usuario lo tenga activado y que permita la inserción de la información GPS en el momento de la toma. Aún así los resultados aportan que la mayoría de las imágenes del banco no posee información GPS (1550 imágenes no y 290 sí).

Además, dentro de este bloque de información se realizará un análisis de las imágenes con información GPS pero que no poseen las etiquetas de latitud y longitud. Cabe destacar que existen imágenes con información GPS, aunque no tengan valor las etiquetas básicas para su posicionamiento. El resultado de este

análisis aporta que en efecto existen 145 imágenes de las 290 que tienen información en alguno de los campos de *GPS Info* y que no tienen la información básica de latitud y longitud. Con *Advanced Query* se ha detectado que 144 de las imágenes pertenecen al móvil LG KU990i y que una pertenece al modelo Sony Ericcson Satio. Con respecto al modelo LG KU990i en sus especificaciones técnicas se indica que no posee sistema GPS, aún así almacena en todas las imágenes la etiqueta *GPSVersionID* con valor "Version 2.3", que no es obligatorio si no hay información GPS. El Sony Ericcson Satio sí posee GPS (concretamente un A-GPS) y almacena las etiquetas *GPSVersionID* con valor "0.0", *GPSAltitudeRef* con valor "Sea level" y *GPSAltitude* con valor "0". Este último caso puede ser debido a que la fotografía se tomó con el sistema A-GPS desactivado o que el usuario no permitió la inserción de información GPS en la imagen. Aun así carece de sentido rellenar las tres etiquetas anteriores con valores aparentemente erróneos.

6.4. Análisis de la información de *thumbnail*

En este apartado se analizan las etiquetas Exif que se encuadran en el bloque *Thumbnail Info*. Primeramente con Query Set se examinarán cuales son las imágenes que no poseen información en este bloque. El resultado de este análisis revela que la mayoría (1437) posee información de *thumbnail*, frente al resto (403), que no la posee.

Cabe destacar otro análisis para identificar el modo de compresión del *thumbnail*, ya que aunque la imagen sea JPEG comprimida, el *thumbnail* puede no estarlo. El resultado de este análisis muestra que el *thumbnail* de todas las imágenes está en formato comprimido JPEG.

6.5. Análisis de la información *Maker Note*

En este apartado se analizan las etiquetas Exif que se encuadran en el bloque *Maker Note Info*. Primeramente con *Query Set* se examinarán cuales son las

imágenes que no poseen información en este bloque. El resultado de este análisis muestra que el 100% de las imágenes no poseen información *Maker Note Info*. Esto puede revelar que en los dispositivos móviles los fabricantes no insertan ningún tipo de información propia, aunque esta afirmación requiere de un estudio a fondo antes poder realizar una extrapolación a todo el conjunto de dispositivos móviles.

6.6. Análisis de la información de Interoperabilidad

En este apartado se analizan las etiquetas Exif que se encuadran en el bloque *Interoperability Info*. Primeramente con *Query Set* se examinarán cuales son las imágenes que no poseen información en este bloque. El resultado de este análisis aporta que 1068 imágenes contienen este tipo de información, frente a 772 que no.

7. CONCLUSIONES Y TRABAJOS FUTUROS

Mediante el uso de la herramienta desarrollada se han utilizado diversas técnicas para realizar estudios sobre los metadatos Exif de un banco propio imágenes. Primeramente cabe destacar como se ha indicado en puntos anteriores, que el banco de imágenes utilizado no es ni mucho menos una muestra de todo el universo de marcas y modelos de dispositivos móviles que existen en la actualidad. Aun dicho esto, se estima que el banco es bastante heterogéneo y numeroso, por lo que los resultados obtenidos puedan ser tenidos en cuenta en futuros trabajos.

La identificación de la fuente de adquisición de la imagen con los metadatos, depende totalmente de que el fabricante inserte los datos respectivos o no. Aún así podemos concluir, por el resultado de los estudios realizados, que en la inmensa mayoría de los casos examinados ha habido éxito. Dada la alta vulnerabilidad de los metadatos a manipulaciones, entendemos que se necesitan técnicas específicas más robustas para la identificación de la fuente basadas en el contenido de la propia imagen y no en sus metadatos. No obstante los metadatos aportan información útil para el analista forense como por ejemplo la relacionada con el geoposicionamiento, la cual actualmente es imposible inferir mediante el contenido de la imagen. Por tanto concluimos que las técnicas de análisis forense que tratan los metadatos Exif pueden servir de apoyo a otras basadas en el contenido de la imagen.

Asimismo, se han mostrado algunos ejemplos de las anomalías detectadas tras el análisis binario manual de las imágenes, no siendo las únicas, ya que se han encontrado otras etiquetas con anomalías como *Exif version*, *Meetering Mode*, *Exposure Program*, *DateTimeOriginal*, etc. Por tanto, se puede concluir que muchos de los fabricantes no siguen fielmente la especificación Exif, indicando lo contrario en el propio archivo, lo que puede producir graves problemas en la extracción de los metadatos de las imágenes por medio de aplicaciones, así como problemas de interoperabilidad entre distintos dispositivos.

7.1. Trabajo Futuro

El trabajo por realizar se enfoca principalmente en la aplicación de técnicas para la identificación de la fuente basadas en el contenido de la imagen. Este trabajo se puede dividir en:

- Estudio en profundidad de las técnicas de identificación de la fuente de imágenes basadas en el contenido para fotografías generadas por DSCs [15] [16] [17] [21] [22] [23] [24] [25] [26] [27] [28]. Tras el estudio aplicar directamente las que puedan ser factibles para imágenes de dispositivos móviles. Adaptación de las técnicas anteriormente aplicadas para el caso específico de imágenes de móviles.

  Sin haber entrado en gran profundidad a su estudio, a priori dado la baja calidad de los sensores CMOS de las cámaras de dispositivos móviles pueden ser técnicas potencialmente útiles las basadas en la aberración de las lentes, las basadas en el uso de las imperfecciones del sensor y las basadas en el uso de las características de las imágenes.

  A priori las técnicas basadas en el proceso de interpolación CFA no serían interesantes para la adaptación al caso de imágenes generadas por dispositivos móviles, dado que los estudios no aportan buenos resultados para distinción entre los distintos modelos de la misma marca y cuando en la imagen se producen procesos de compresión (como el que se da en JPEG).

- Estudio en profundidad de las técnicas de identificación de la fuente de imágenes basadas en el contenido para fotografías generadas por dispositivos móviles [12] [14] [29] [30]. Tras el estudio modificar las técnicas que se consideren que pueden obtener los mejores resultados.

REFERENCIAS

[1] J. Hsu: "The Worldwide Mobile Phone Camera Module Market and Taiwan's Industry, 2009 and Beyond", *Market Intelligence & Consulting Institute (MIC)*, 2009

[2] Infotrends: "Worldwide Camera Phone Forecast: 2007-2012", *Weymouth, MA: Infotrends*, 2008.

[3] Richard L. Baer: "Resolution Limits in Digital Photography: the Looming End of the Pixel Wars", *Imaging Systems, OSA technical Digest (CD) (Optical Society of America, 2010)*, paper ITuB3. http://www.opticsinfobase.org/abstract.cfm?URI=IS-2010-ITuB3

[4] L. Srivastava: "Mobile phones and the evolution of social behavior", *Behaviour & Information Technology*, Vol. 24, No. 2, pp. 111 – 129, 2005.

[5] T. Gloe, M. Kirchner, A. Winkler, R. Böhme: "Can We Trust Digital Image Forensics?", *in Proceedings of the 15th international conference on Multimedia (MM'07)*, Augsburg, Bavaria, Germany, September 23–28, pp. 78–86. ACM Press, New York, 2007.

[6] T.V. Lanh, K. Chong, S. Emmanuel, M.S. Kankanhalli: "A survey on digital camera image forensic methods", *in proceedings of IEEE International Conference on Multimedia and Expo*, pp. 16–19, 2007.

[7] V. Thing, K.-Y. Ng, E. Chang: "Live memory forensics of mobile phones", *Digital Investigation*, Vol. 7, pp. S 74-82, 2010.

[8] N. Romero, V. Gimenez, J. Serrano, A. Selles, F. Canet, M. Cabrera: "Recovery of descriptive information in images from digital libraries by means of EXIF metadata", *Library Hi Tech*, Vol. 26 No. 2, pp.302 – 315, 2008.

[9] M. Boutell, J. Luo: "Photo classification by integrating image content and camera metadata", *in Proceedings of the 17th International Conference on Pattern Recognition (ICPR '04)*, Vol. 4, pp. 901–904, 2004.

[10] J. Tesic: "Metadata Practices for Consumer Photos", *IEEE Multimedia,* Vol. 12, No. 3, pp.86-92, 2005.

[11] C. McKay, A. Swaminathan, H. Gou, M. Wu: "Image acquisition forensics: Forensic analysis to identify imaging source", *in Proceedings of the 2008 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2008)*, pp. 1657–1660, 2008.

[12] O. Çeliktutan, B. Sankur, I.Avcibas: "Blind identification of source cell-phone model", *IEEE Transactions on Information Forensics and Security*, Vol. 3, No. 3, pp. 553–566, 2008.

[13] H. Cao, A.C. Kot: "Accurate Detection of Demosaicing Regularity for Digital Image Forensics", *IEEE Transactions on Information Forensics and Security*, Vol. 4, No. 4, pp. 899 – 910, 2009.

[14] M. J. Tsai, C. L. Lai, J. Liu: "Camera/mobile phone source identification for digital forensics", *in Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2007)*, pp. II 221–224, 2007.

[15] K.S. Choi, E.Y. Lam, K.Y. Wong: "Automatic Source Identification Using the Intrinsic Lens Radial Distortion", *Optics Express*, Vol. 14, No. 24, pp. 11551-11565, 2006.

[16] E. Dirik, H. T. Sencar, N. Memon: "Source camera identification based on sensor dust characteristics", *in Proceedings of IEEE Workshop on Signal Processing Applications Public Security Forensics*, Apr. 11–13, pp. 1–6, 2007.

[17] Y. Long, Y. Huang: "Image based source camera identification using demosaicking", *in Proceeding of IEEE 8th Workshop Multimedia Signal Processing*, pp. 419–424, 2006.

[18] I. Avcıbaş, M. Kharrazib, N. Memon, B. Sankur: "Image Steganalysis with Binary Similarity Measures", *EURASIP Journal of Applied Signal Processing*, No. 17, pp. 2749–2757, 2005.

[19] I. Avcıbaş, N. Memon, B. Sankur: "Steganalysis using image quality metrics", *IEEE Transactions on Image Processing*, Vol. 12, No. 2, pp. 221–229, 2003.

[20] S. Lyu, H. Farid: "Steganalysis using higher-order image statistics", *IEEE Transactions on Information Security and Forensics*, Vol. 1, No. 1, pp. 111–119, 2006.

[21] K. S. Choi, E. Y. Lam, K. K. Y. Wong: "Source camera identification using footprints from lens aberration", *in proceedings of SPIE Digital Photography II*, Vol. 6069, pp. 172–179, 2006.

[22] Z. Geradts, J. Bijhold, M. Kieft, K. Kurosawa, K. Kuroki, N. Saitoh: "Methods for identification of images acquired with digital cameras", *in proceedings of Enabling Technologies for Law Enforcement and Security*, Vol. 4232, pp. 505–512, 2001.

[23] J. Lukas, J. Fridrich, M. Goljan: "Digital camera identification from sensor pattern noise", *IEEE Transactions on Information Forensics and Security*, Vol. 1, No. 2, pp. 205–214, 2006.

[24] S. Bayram, H. Sencar, N. Memon, I. Avcibas: "Source Camera Identification Based on CFA Interpolation", *in proceedings of the IEEE International Conference on Image Processing*, pp. 69–72, 2005.

[25] Y. Long, Y. Huang: "Image based source camera identification using demosaicking", *in proceedings of IEEE 8th Workshop Multimedia Signal Processing*, pp. 419–424, 2006.

[26] M. Kharrazi, H.T. Sencar, N. Memon: "Blind Source Camera Identification", *in proceeding of International Conference on Image Processing (ICIP 2004)*, Singapore, October 24–27, 2004.

[27] M. Boutell, J. Luo. "Beyond: pixels: Exploiting camera metadata for photo classification", *Pattern Recognition,* Vol. 38 No. 6, pp. 935-946, 2005.

[28] Sevinc Bayram, Husrew T. Sencar, Nasir Memon: "Improvements on source camera-model identification based on CFA interpolation", *in proceedings of WG 11.9 International Conference on Digital Forensics*, Orlando, FL, pp. 24–27, 2006.

[29] C.-L. Lai, Y.-Sh. Chen: "The application of intelligent system to digital image forensics", *in proceedings of the Eight International Conference on Machine Learning and Cybernetics*, pp. 2991 – 2998, 2009

[30] V. T. Lanh, S. Emmanuel, M. S. Kankanhalli: "Identifying source cell phone using chromatic aberration", *in proceedings of IEEE International Conference on Multimedia and Expo*, pp. 883 – 886, 2007.

[31] M. Al Zarouni: "Mobile handset forensic evidence: a challenge for law enforcement", *in proceedings of 4th Australian Digital Forensics Conference*, Perth, Western Australia, pp 1 -10, 2006.

[32] Wessttek. ClearVue Suite. http://www.westtek.com/smartphone/

[33] O. Celiktutan, I. Avcibas, B. Sankur, N. Memon: "Source Cell-phone Identification", *IEEE Signal Processing and Communications Applications*, pp. 1-3, 2005.

[34] Metadata Working Group.
http://www.metadataworkinggroup.org/pdf/mwg_guidance.pdf

[35] Exchangeable Image File for digital still cameras: Exif version 2.3
http://www.cipa.jp/english/hyoujunka/kikaku/pdf/DC-008-2010_E.pdf

[36] Adobe Developers Association. 1993
http://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf.

[37] C. Hamilton, C. Cube: Microsystems. JPEG File Interchange Format. Version 1.02, September 1, 1992.
http://www.w3.org/Graphics/JPEG/jfif3.pdf.

[38] International Press Telecomunications Council. http://www.iptc.org

[39] Extensible Metadata Platform. http://www.adobe.com/products/xmp

[40] Exif Jpeg header manipulation tool.
http://www.sentex.net/~mwandel/jhead/

[41] ExifTool. http://www.sno.phy.queensu.ca/~phil/exiftool/

[42] Exif Viewer 1.60.
https://addons.mozilla.org/es-es/firefox/addon/exif-viewer/

[43] ExifPro Image Viewer
http://www.exifpro.co

A. ESPECIFICACIÓN DE LA HERRAMIENTA

A continuación se va a realizar una presentación pormenorizada de la aplicación desarrollada. Como se comentó en el capítulo 5 la herramienta se divide en dos grandes partes: tratamiento de fotos a nivel individual y tratamiento de fotos a nivel de grupo.

A.1. Tratamiento de fotos a nivel individual

Esta funcionalidad está asociada a la pestaña *Exif Info* y su apariencia gráfica general puede verse en la figura 28.

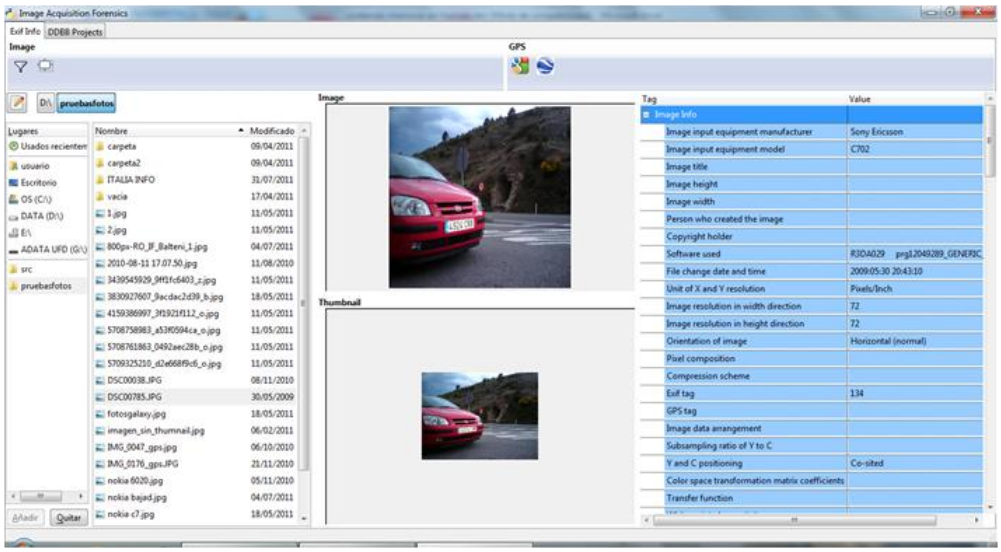


Fig. 28. Apariencia general de la pestaña *Exif Info*

Como estructura general se puede apreciar a la izquierda de la imagen un navegador de archivos, en el centro la imagen del archivo seleccionado y su correspondiente *thumbnail* (es el incluido en el propia archivo de la imagen no ninguna generación propia del programa) y a la derecha las etiquetas Exif con su correspondiente información. De esta estructura cabe destacar en la interfaz gráfica que es totalmente configurable a nivel de tamaños, es decir todos los separadores entre las distintas zonas se pueden mover.

Una vez descrita la pantalla principal a grandes rasgos se va a presentar cada una de las opciones y funcionalidades en profundidad.

- **Navegador de archivos**: Cuando un archivo de una imagen es seleccionado se muestra su imagen, su *thumbnail* (si lo posee) y toda la información Exif que ha podido ser extraída. Asimismo cabe destacar que si existe algún tipo de error en la apertura de imagen, *thumbnail* o el análisis sintáctico de los datos Exif, los correspondientes apartados aparecerán vacíos y se indicará el error mediante el pertinente mensaje. Un ejemplo de apertura errónea de un archivo que no es una imagen se muestra en la figura 29.

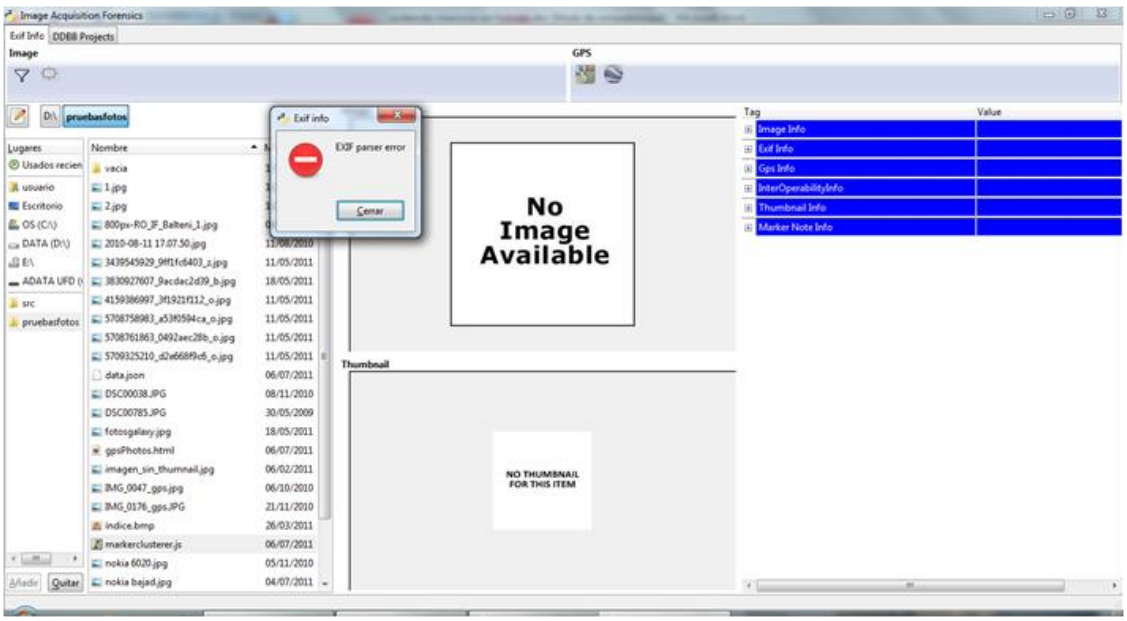


Fig. 29. Apertura errónea de un archivo

Además se permite almacenar y borrar los directorios de uso más común para facilitar el acceso a rutas. Para ello simplemente hay que seleccionar la ruta deseada y pulsar el botón "Añadir". Para eliminar la ruta almacenada solo hay que seleccionarla y pulsar el botón "Quitar". Un ejemplo de esta funcionalidad se muestra en la figura 30.

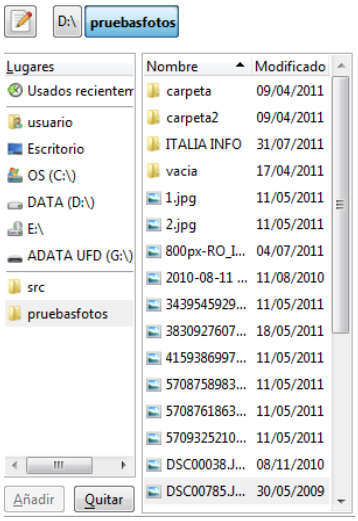


Fig. 30. Tratamiento de rutas

- **Menú *Image***: Posee dos opciones: una para filtrar el tipo de archivos que se muestran en el navegador de imágenes y otra para cambiar el tamaño de la imagen y el *thumbnail* a mostrar.

- **Menú *GPS***: Se utiliza para sacar partido a los datos de geoposicionamiento que pueden ser incluidos en las imágenes. Si la imagen no tiene la suficiente información para poder ser mostrada en alguna de las opciones al pulsarla se mostrará un mensaje indicándolo (*Not enought GPS information*).

  Dentro de este menú existen dos opciones: posicionamiento en Google Maps y en Google Earth. En la primera se abrirá el navegador web por defecto del sistema operativo y se mostrará la ubicación inserta en los metadatos de la imagen en un mapa de Google Maps (es necesario conexión a internet). La figura 31 muestra un ejemplo de geoposicionamiento en una fotografía en Google Maps.

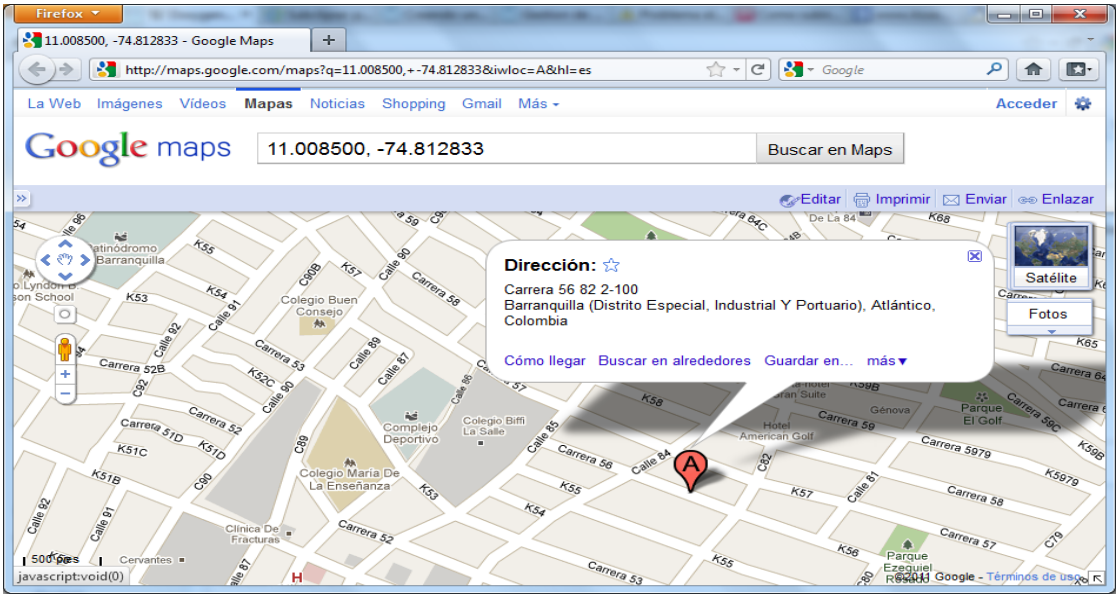


Fig. 31. Geoposicionamiento en Google Maps

En la segunda opción se abrirá un menú (figura 32) para poder almacenar un archivo de extensión "kml". Este archivo podrá ser posteriormente abierto si está instalada la aplicación Google Earth, en la cual se mostrará igualmente la posición geográfica almacenada en los metadatos de la imagen (es necesario conexión a internet).

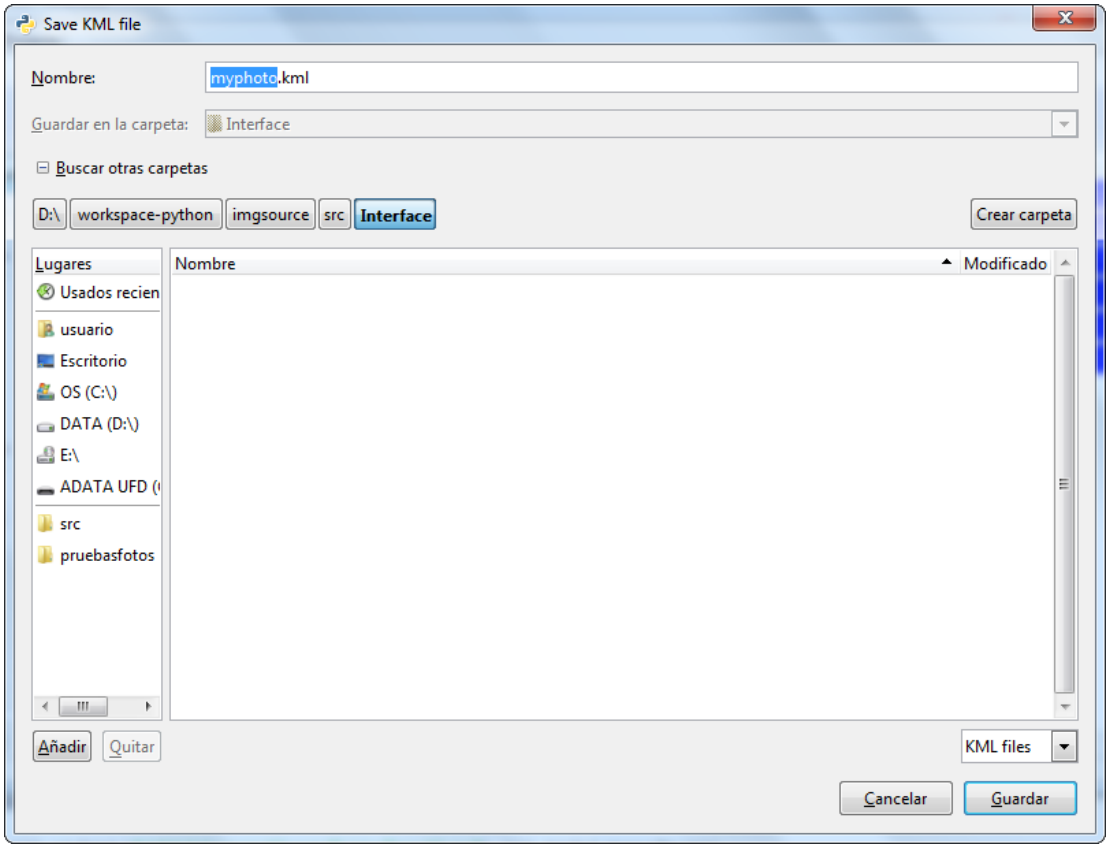


Fig. 32. Almacenamiento de archivos KML

La figura 33 muestra un ejemplo de geoposicionamiento de una fotografía en Google Earth.

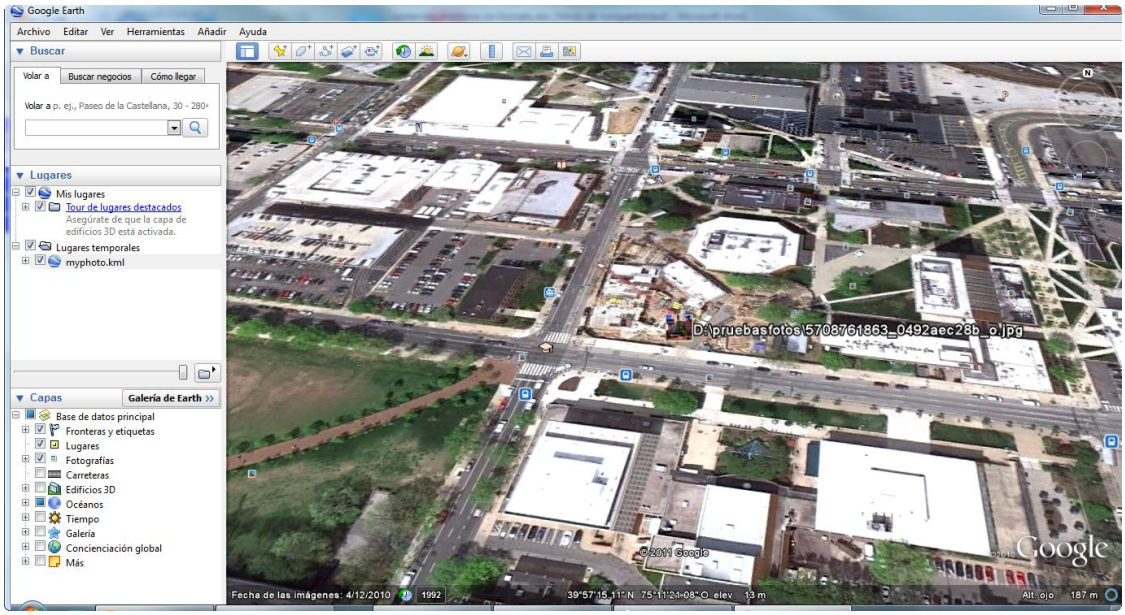


Fig. 33. Geoposicionamiento con Google Earth

- **Vista de imagen y *thumbnail***: Muestra la imagen y el *thumbnail* del archivo seleccionado en el navegador de archivos. Este bloque posee barras de desplazamiento horizontal y vertical por si la alguna de las imágenes es mayor que el tamaño que el usuario ha seleccionado para este espacio.

- **Etiquetas Exif**: En este bloque se muestran todos los metadatos Exif obtenidos del archivo seleccionado en el navegador de archivos. Se muestra la etiqueta y su correspondiente valor. Siempre se muestran todas las etiquetas que la aplicación captura, si una etiqueta no tiene valor para una imagen se muestra con valor vacío.

  También se destaca que al pasar el ratón sobre el valor de una etiqueta aparece un menú contextual con una descripción orientativa basada en la propia especificación Exif 2.3. Como puede apreciarse en la figura 34 para mostrar la información se han creado 6 grupos: *Image*, *Exif*, *GPS*, *Interoperability*, *Thumbnail* y *Maker Note*.

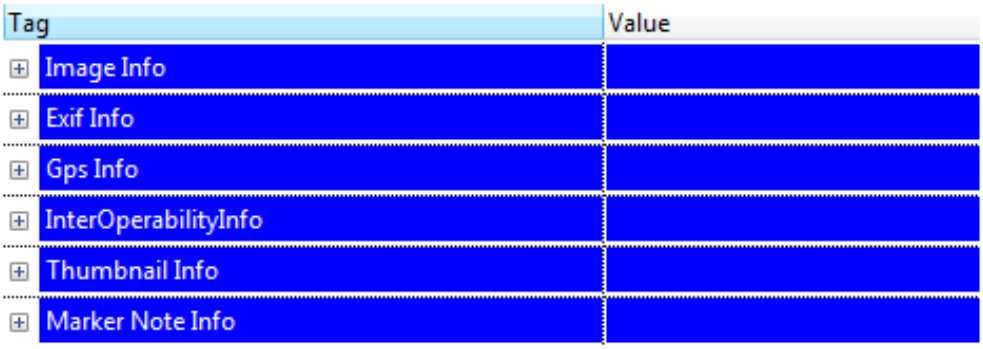


Fig. 34. Grupos de etiquetas Exif

A continuación se va a describir de forma general la información que aporta cada uno de los grupos:

- ***Image Info***: En este bloque se almacenan las etiquetas con información relativa a la propia imagen y que no tienen relación directa con el entorno y el momento de la captura. Por ejemplo la marca y modelo de la cámara,

el tamaño de la imagen, la unidad utilizada en la resolución X e Y, etc.

- ***Exif Info*:** En este bloque se guardan las etiquetas con información relativa al momento o al entorno de la toma de la imagen. Dentro de este bloque se encuentra por ejemplo la información referente al flash, hora de toma y generación de la imagen, configuración de la lente, etc.

- ***GPS Info***: En este bloque está toda la información relativa al geoposicionamiento. Por ejemplo información de latitud, longitud, altitud, el estado del receptor GPS, etc.

- ***InterOperability Info***: En este bloque se incluyen las etiquetas relativas a la información de las reglas de interoperabilidad, como pueden ser *Exif R98*, *DCF thumbnail file* o *DCF Option file*.

- ***Thumbnail Info***: En este bloque se encuentran todas las etiquetas relativas a la información de *thumbnail*. Por ejemplo su tamaño en vertical y horizontal y el esquema de compresión utilizado.

- ***Maker Note Info*:** Es una etiqueta individual que almacena la información que cada fabricante puede insertar de forma opcional y que no ha sido recogida en ninguna etiqueta Exif.

  El formato de esta información es libre y no tiene una estructura prefijada, cada fabricante utiliza la suya propia que incluso puede ser diferente para distintos modelos de la misma marca. Por tanto se muestra como una secuencia de bytes (en hexadecimal). Si se conoce la estructura estos bytes pueden ser decodificados de forma manual.

A.2. Tratamiento de imágenes a nivel de grupo

Esta funcionalidad está asociada a la pestaña *DDBB Projects* y su apariencia gráfica general puede verse en la figura 35.

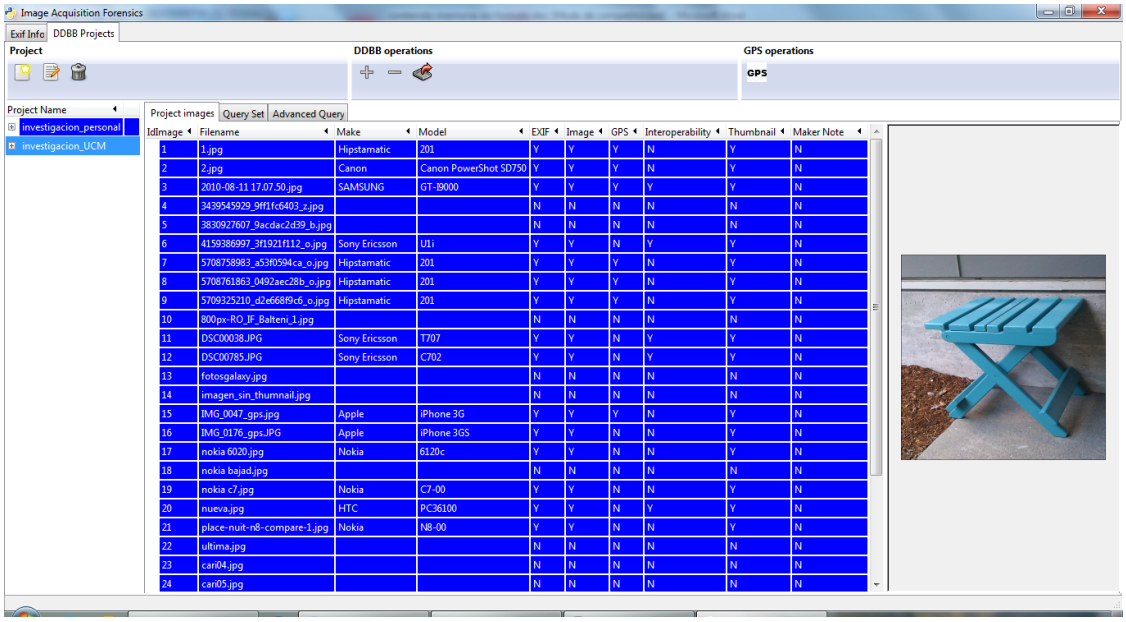


Fig. 35. Apariencia general de la pestaña *DDBB Projects*

La estructura de esta funcionalidad es mucho más compleja que la de la pestaña *Exif Info*. Asimismo ofrece gran diversidad de opciones al analista forense.

Lo primero a destacar en esta funcionalidad es que la imágenes se tratan en grupos llamados proyectos. Estos grupos pueden ser de una o más imágenes. Cada proyecto es totalmente independiente entre sí. Se busca acercar la realidad del día a día del analista forense a la herramienta, es decir, el analista tendrá diversos casos de análisis disjuntos los cuales podrá tratar en proyectos distintos.

Dentro de esta pestaña se va a mostrar en profundidad las siguientes funcionalidades: gestión de proyectos, administración de imágenes de los proyectos, consultas en conjunto (*query set*), consultas avanzadas (*advanced query*) y geoposicionamiento de las imágenes.

A.2.1. Gestión de proyectos

La gestión de proyectos se corresponde con el menú *Project*. Éste tiene las opciones de creación, edición y borrado de proyectos.

- **Creación de proyectos**. Al pulsar sobre la creación de proyectos se abre una ventana como la de la figura 36. En esta hay que introducir el nombre del proyecto, el o los formatos de archivos que se quieren incluir (todos los archivos, JPEG o BMP) y la ruta de donde tomar los archivos. Por tanto se creará un proyecto con el nombre indicado, que incluye todos los archivos filtrados según la opción de formato escogida que se encuentren en la ruta seleccionada y en todos sus subdirectorios (de cualquier nivel).

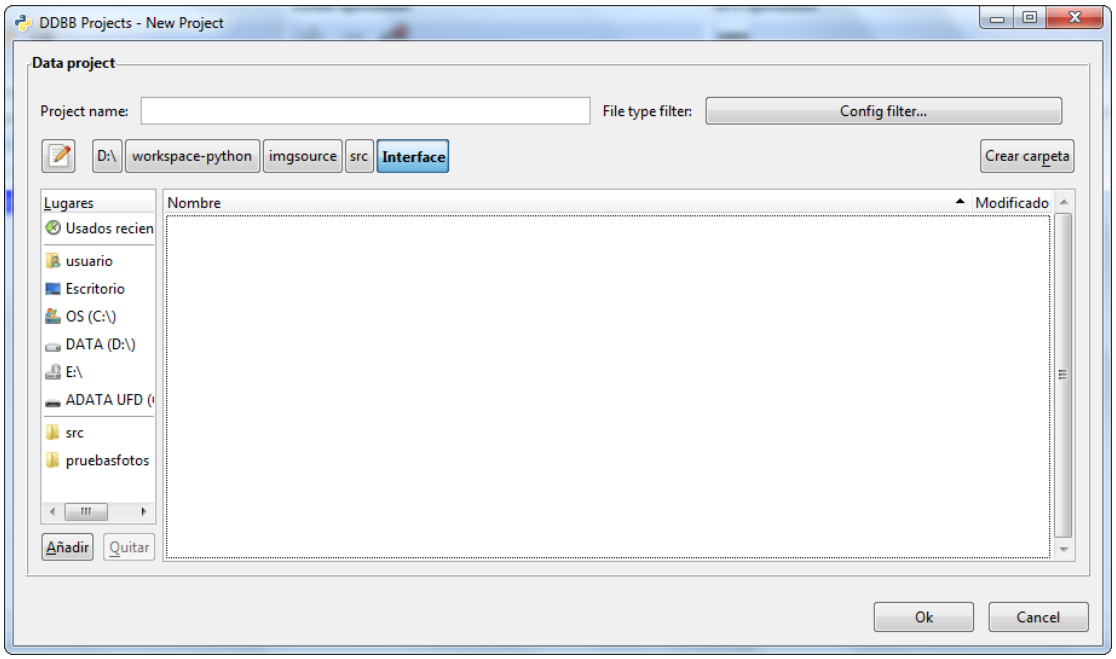


Fig. 36. Creación de Proyectos

Una vez introducido todos los parámetros de forma correcta se creará el nuevo proyecto mostrándose en el bloque de la izquierda. Además del nombre del proyecto, se mostrará su fecha de creación y la carpeta base de donde se tomaron los archivos. Es muy importante destacar que en el momento de la creación del proyecto las imágenes se almacenan en una base de datos interna de la aplicación. Esta base de datos es totalmente independiente del directorio y no existe sincronización alguna con él, sólo se muestra la ruta de donde se cargaron los datos como información que puede ser de ayuda. Es decir y haciendo hincapié, una vez creado el proyecto no hay relación alguna entre las imágenes de la base de datos de

la aplicación y las imágenes del soporte físico de donde han sido extraídas.

Cuando se pulsa el botón aceptar la aplicación va tomando uno a uno los archivos seleccionados y obteniendo sus metadatos para cargarlos en la base de datos interna. Si hay algún tipo de problema en el tratamiento de los archivos (archivos que no son imágenes, problemas con los permisos del sistema operativos, errores en el análisis sintáctico, etc.) la aplicación generará una lista con los archivos que no han podido ser incluidos en la base de datos y la razón de su no inclusión. Si todos los archivos han sido incluidos en la base de datos de manera exitosa está lista no será mostrada.

En la figura 37 se muestra un ejemplo de la forma de presentar la información de un proyecto.

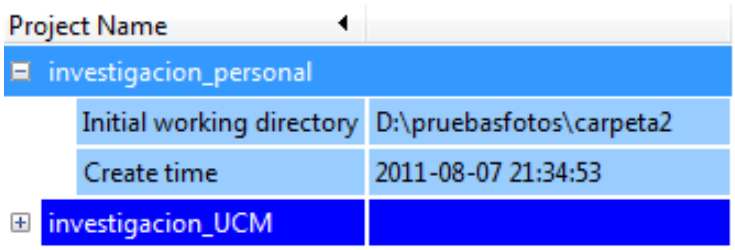


Fig. 37. Información de proyectos

- **Edición de proyectos**. Permite editar el nombre del proyecto. La figura 38 muestra la pantalla de Edición de proyectos.

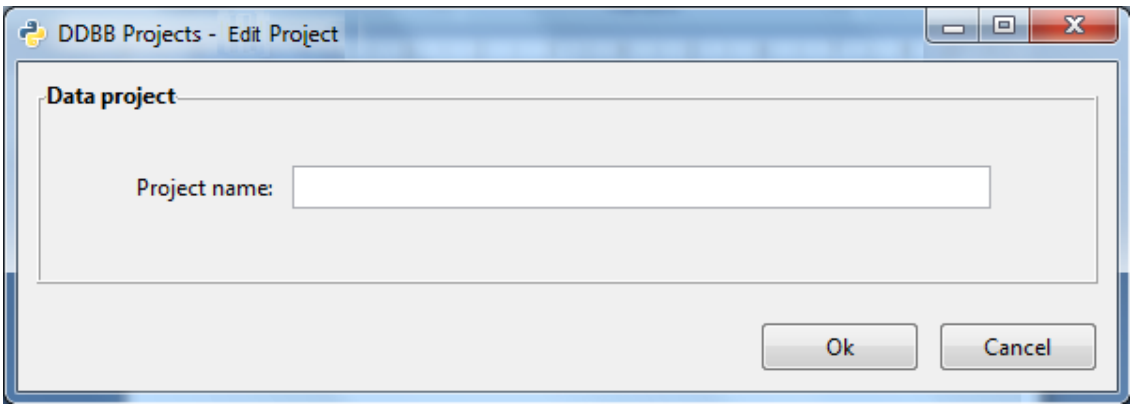


Fig. 38. Edición de proyectos

- **Borrado de proyectos**: Permite eliminar el proyecto seleccionado. Se mostrará un mensaje de confirmación antes de realizarse el borrado final. Una vez borrado el proyecto será imposible recuperarlo.

A.2.2. Administración de imágenes de los proyectos

La administración de imágenes de cada uno de los proyectos se realiza con el menú *DDBB Operations*. Dentro de este menú se encuentran las opciones de añadir y eliminar imágenes de un proyecto, visualización de las imágenes de un proyecto y exportarlas a un directorio.

- **Añadir imágenes a un proyecto**: El añadir imágenes a un proyecto es análogo a la creación de un nuevo proyecto, salvo que como es evidente el nombre del proyecto no se puede editar. Cabe destacar que en un mismo proyecto puede haber dos imágenes con el mismo nombre y contenido. Es decir, en un proyecto puede estar el mismo archivo incluido varias veces. Este caso se permite ya que un analista forense puede querer examinar un dispositivo que al él no le pertenece y en este puede estar el mismo archivo repetido varias veces en distintas ubicaciones. La figura 39 muestra la pantalla para añadir fotografías a un proyecto.

  Si durante el proceso se presentan errores, se insertan en el proyecto creado las fotos que están correctas y se muestra un informe de los ficheros que no se pudieron agregar al proyecto y la causa para cada uno de ellos.

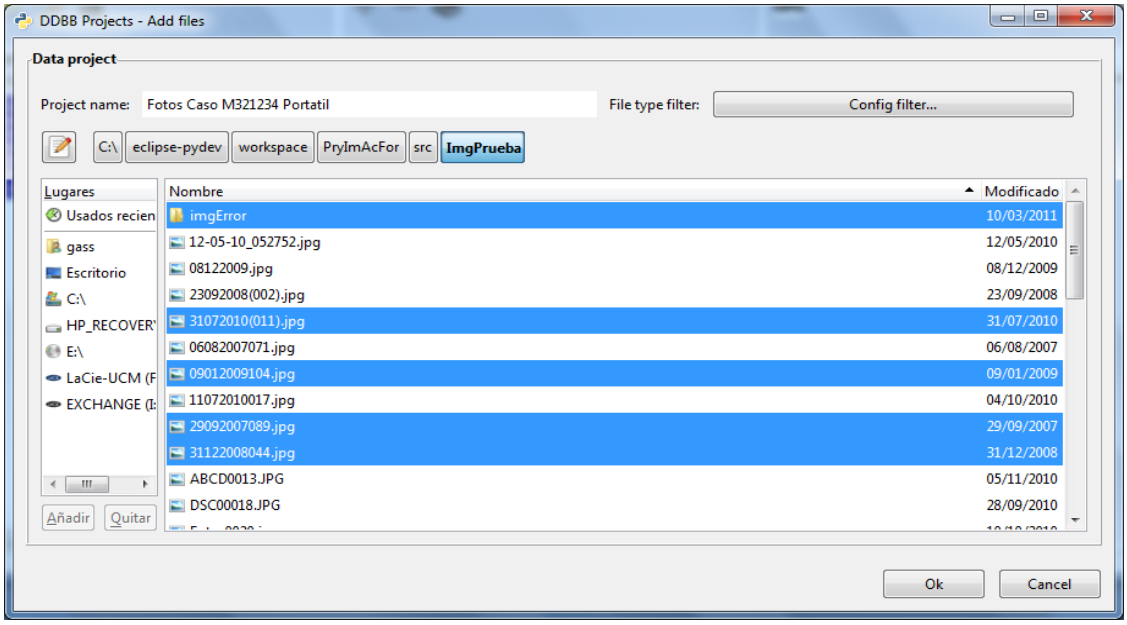


Fig. 39. Añadir imágenes a proyectos

- **Eliminar imágenes de un proyecto**: Al pulsar este botón se abre una ventana con una lista de todas las imágenes del proyecto para poder seleccionar una o varias imágenes y proceder a su eliminación. Si se seleccionan las imágenes una a una además se muestra el contenido de la misma. La figura 40 muestra la pantalla de eliminación de imágenes de un proyecto.

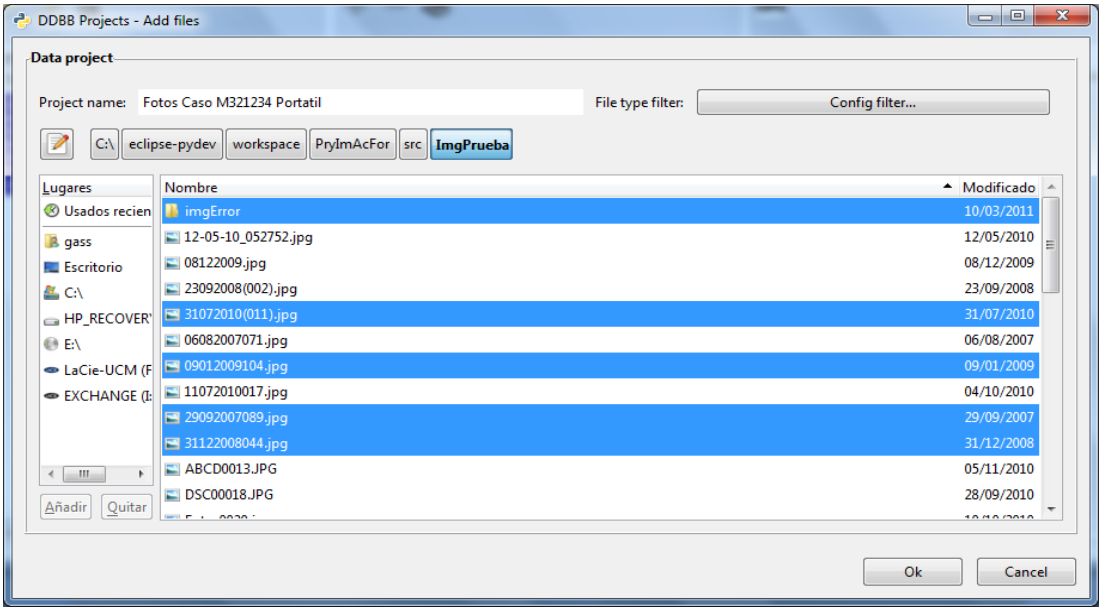


Fig. 40. Eliminar imágenes de proyectos

- **Visualización de las imágenes de un proyecto**: En la parte central de la pestaña *DDBB Projects* y dentro de ésta en la pestaña *Project Images* se muestran una lista de las imágenes del proyecto seleccionado en la lista de proyectos.

  Para cada imagen se muestra su identificador interno de la base de datos (para permitir el caso de archivos con el mismo nombre), el nombre del archivo, la marca y el modelo de dispositivo que la creó (si existe). Además se presenta la información de si posee metadatos en los distintos grupos Exif que analiza la herramienta. Asimismo se visualiza el contenido de cada una de las imágenes a la derecha según se van seleccionando. Un ejemplo de captura de esta funcionalidad se muestra en la figura 41.

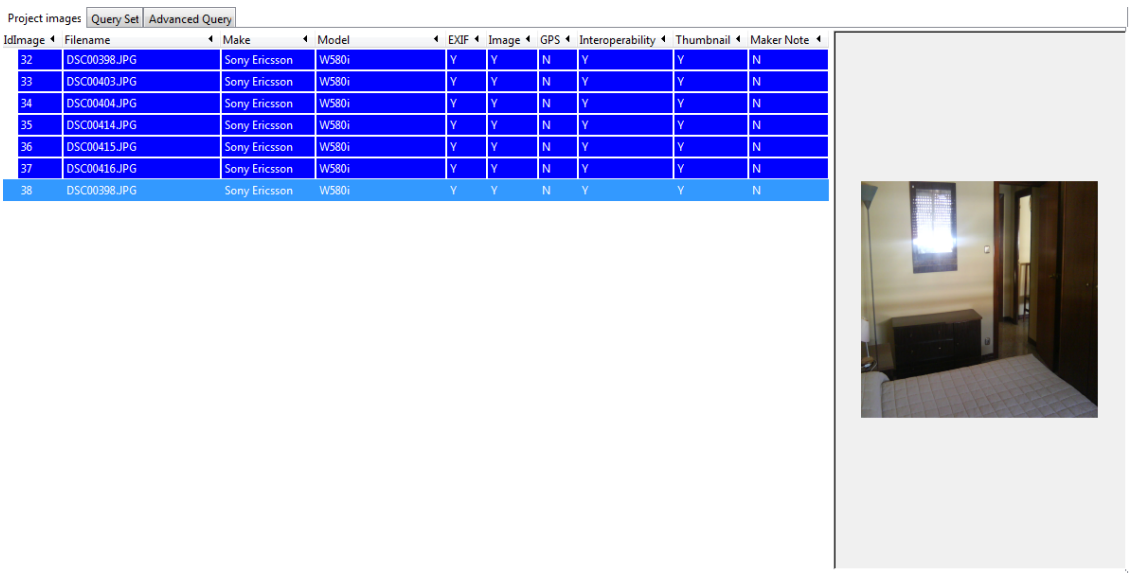


Fig. 41. Visualización de las imágenes de un proyecto

- **Exportar las imágenes de un proyecto**: Esta opción permite exportar un grupo de archivos de un proyecto a una ruta seleccionada por el usuario.

A.2.3. Consultas en conjunto (*Query Set)*

La funcionalidad de consultas en conjunto (*Query Set*) se encuentra en la

pestaña *Query Set* de la pestaña principal *DDBB Projects*. En esta opción se permite crear consultas agregando etiquetas Exif (y otros adicionales que añade la aplicación) sobre las imágenes del proyecto seleccionado. Un ejemplo de apariencia general puede verse en la figura 42.

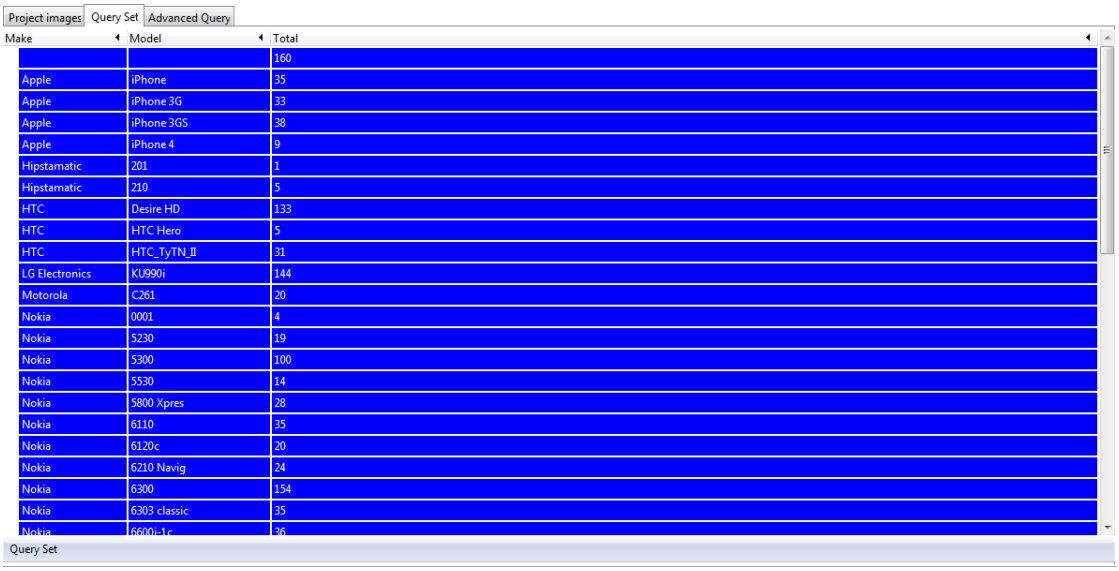


Fig. 42. Query Set

En las consultas permiten escoger 5 campos de agregación como máximo (por defecto se realiza sobre *Make* y *Model*, aunque ser pueden elegir cualesquiera). Para escoger los distintos campos hay que pulsar sobre el botón *Query Set* y aparecerá la ventana de la figura 43.

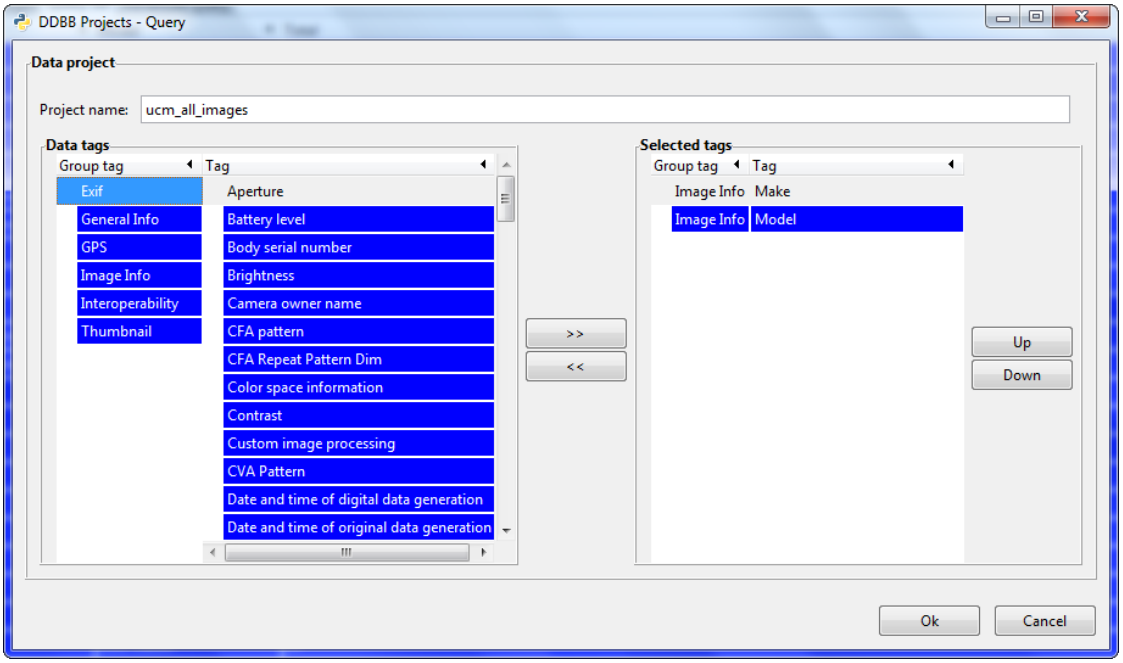


Fig. 43. Selección de campos de agregación

En la figura 44 se pueden escoger cualquiera de las etiquetas Exif de los distintos grupos que trata la aplicación (Exif *Info*, *General Info*, *GPS*, *Image Info*, *Interoperability* y *Thumbnail*). Además se puede elegir un grupo adicional de información general *General Info*, en el cual se han incluido nuevos campos que se consideran interesantes para este tipo de consultas. Los campos incluidos en el grupo *General Info* son: fecha de creación de la imagen, ruta de origen de la carga de la imagen, identificador interno de la base de datos, nombre de archivo, proyecto al que pertenece, formato del archivo y si posee información para cada uno de los grupos *Exif Info, GPS Info, Image Info, Interoperability Info, Maker Note* y *Thumbnail*. Una vez escogidos los campos, se puede modificar el orden en el que quieren ser mostrados en el resultado, para ello se utilizarán los botones "*Up*" y "*Down*". Finalmente para ejecutar la consulta pulsar "*Ok*" y aparecerá el resultado en la ventana inicial de *Query Set*.

La consulta agrupa las imágenes por los criterios seleccionados y muestra el número de imágenes que hay en cada uno de los grupos formados. Por ejemplo si queremos ver cuántas imágenes hay de cada marca y modelo en un proyecto

se debe seleccionar los campos *Image input equipment manufacturer* e *Image input equipment model* del grupo *Image Info* y pulsamos "*Ok*". El resultado mostrará todas las marcas y modelos de dispositivos móviles que hay en ese proyecto y el número de imágenes de cada uno (ver figura 42).

A.2.4. Consultas avanzadas (*Advanced Query*)

La funcionalidad de consultas avanzadas (*Advanced Query*) se encuentra en la pestaña *Advanced Query* de la pestaña principal *DDBB Projects*. Esta es la funcionalidad más potente y versátil de la herramienta, además de la más completa. Una visión general se muestra en la figura 44.

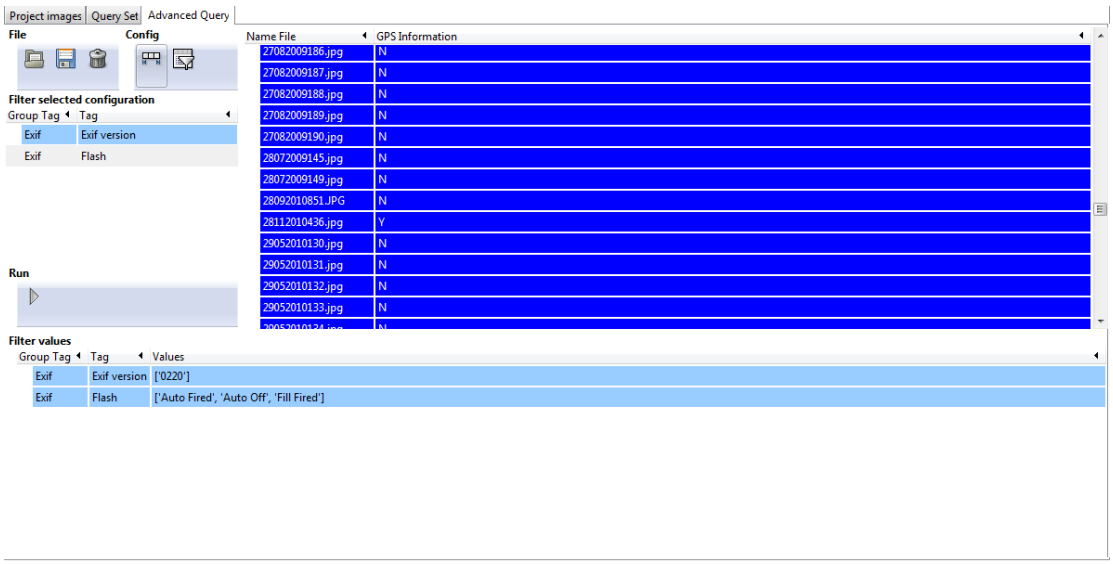


Fig. 44. *Advanced Query*

En *Advanced Query* hay que distinguir dos grandes bloques: la configuración de la consulta y su almacenamiento.

Con respecto a la configuración de la consulta avanzada hay que tener en cuenta la configuración de las columnas de los resultados y la configuración de los filtros. En esta consulta se muestran los valores de los campos seleccionados por la configuración de las columnas de los resultados que cumplen las restricciones indicadas en la configuración de los filtros.

- **Configuración de las columnas de los resultados**: Esta opción se realiza con el botón "*Config Query Columns*" del menú *Config*. Muestra una ventana para selección de los campos que se quieren mostrar como columnas en el resultado de la consulta. Esta ventana tiene el mismo modo de funcionamiento que la utilizada en *Query Set* salvo con la excepción de no tener límite para el número de campos que se pueden escoger en las columnas. Al menos una columna debe ser escogida antes de ejecutar la consulta sino la aplicación lo indicará con un mensaje de error. Una vez seleccionados estos campos se mostrarán como columnas en la parte superior como se muestra en la figura 45.

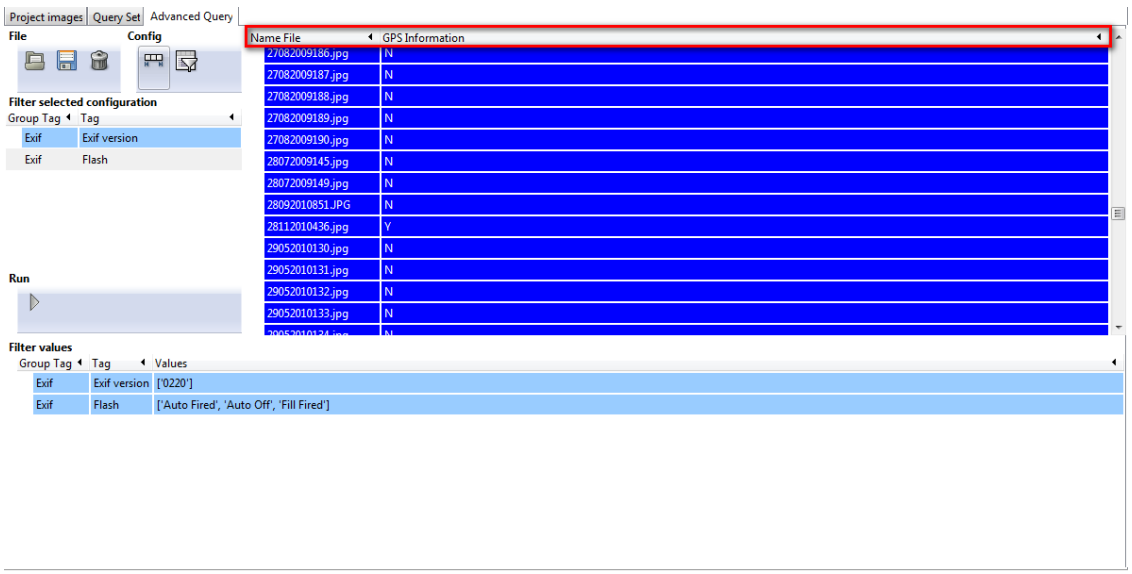


Fig. 45. Configuración de las columnas de resultado

- **Configuración de los filtros**: Para configurar esta opción hay que realizar varios pasos:

  - Seleccionar los campos que se utilizarán como filtros: La ventana de selección de estos campos es análoga a la pantalla de selección de campos para la configuración de las columnas. Una vez elegidos los filtros se incluirán en el bloque *Filter selected configuration* como se aprecia en la figura 46.

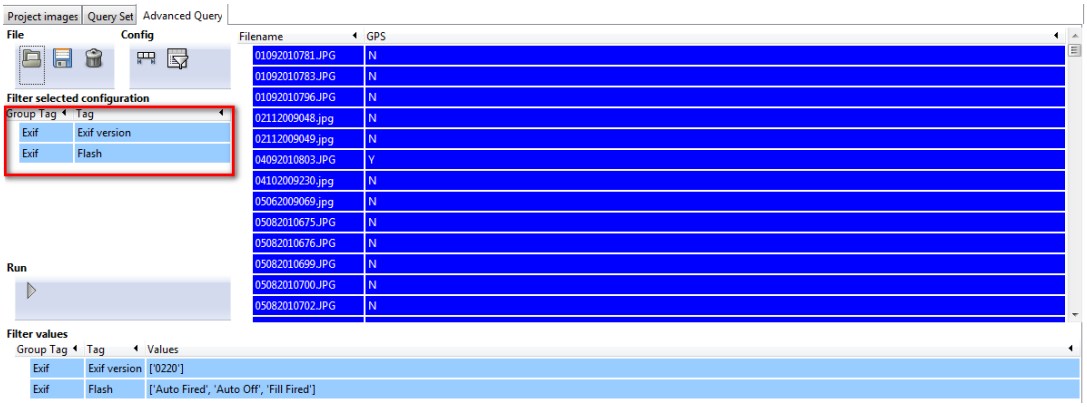


Fig. 46. Configuración de filtros

- Configurar los valores de cada uno de los filtros para ejecutar finalmente la consulta: Si existe algún filtro sin configurar a la hora de ejecutar la consulta se mostrará un mensaje de error indicándolo. Para configurar cada uno de los filtros hay que hacer doble clic en cada uno de ellos en el bloque *Filter selected configuration*. Tras el doble clic aparecerá una ventana con los valores posibles de esa etiqueta para las imágenes del proyecto seleccionado. El analista deberá seleccionar los valores por los que se desea realizar el filtrado. Si seleccionan varios valores para un mismo filtro la imagen debe tener poseer uno de los valores pero no todos, ya que en Exif cada campo solo puede tener un valor y no un conjunto de valores. Por ejemplo si elegimos para filtrar el campo *Exif Flash* y configuramos los valores *Auto Fired* y *Auto Off*, al ejecutar la consulta, se mostrarán los valores de la columnas configuradas de las imágenes que posean en la etiqueta *flash* el valor "*Auto Fired*" o "*Auto Off*". Por tanto en la configuración de los valores de cada uno de los filtros, la aplicación al realizar la consulta hace una O (or) lógica con respecto a los valores seleccionados. En cambio entre los distintos filtros seleccionados la aplicación al realizar la consulta hace una Y (and) lógica entre los distintos campos a filtrar.

Una vez configurada totalmente la consulta para ejecutarla hay que pulsar el botón "*Run query to current project*" y seguidamente se mostrarán los

resultados.

Por ejemplo si queremos obtener el nombre de la imagen y el valor de la latitud de las imágenes que han sido realizadas con flash "*Auto fired*" o "*Fired*" y que además tengan información en algunos de sus campos GPS hay que realizar los siguientes pasos:

1. Configurar las columnas de resultados escogiendo los campos *Name File* y *Latitude*.

2. Seleccionar los filtros *Exif Flash* y *General Info GPS Information*.

3. Configurar los valores de los filtros seleccionados. Para "Exif Flash" tomar los valores "Auto fired" y "Fired" y para "General Info GPS Information" el valor "Y".

4. Pulsar el botón "Run query to current project".

El resultado obtenido para la anterior consulta y un proyecto de prueba se muestra en la figura 47.

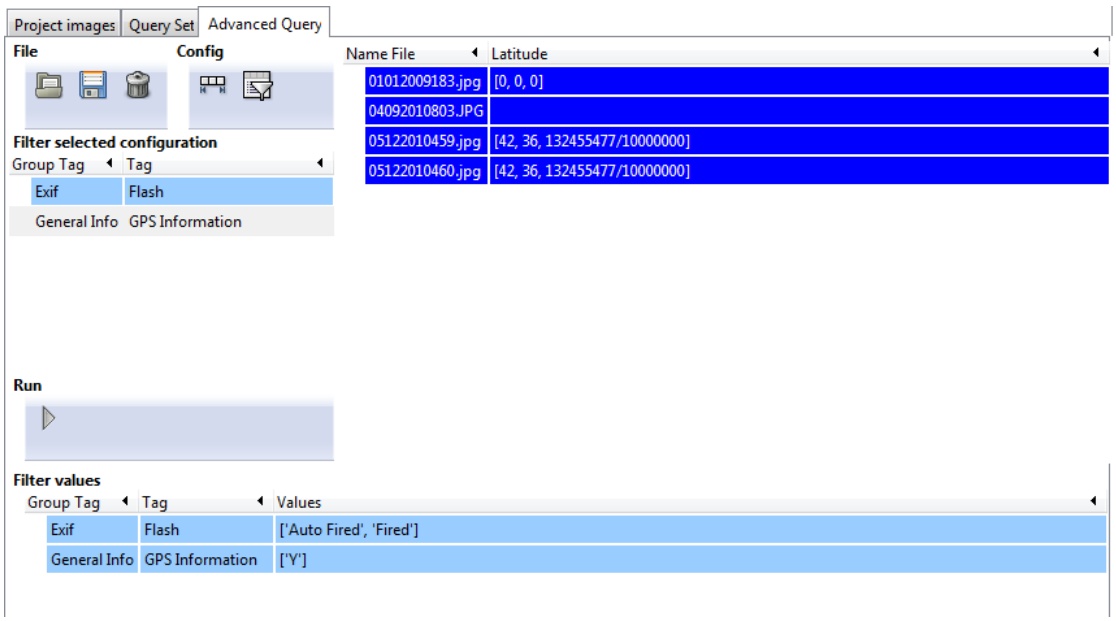


Fig. 47. Ejemplo de resultados de consulta con *Advanced Query*

Se puede observar que existen 4 imágenes que cumplen los criterios y se muestran sus latitudes ([grados, minutos, segundos]). En la segunda imagen de la lista, se puede apreciar que no hay información de latitud. Inicialmente esto puede chocar un poco, ya que uno de los filtros indicaban que tenía que tener información GPS. El resultado es bueno ya que esa imagen posee información GPS en otras etiquetas pero posee la etiqueta de la latitud vacía.

La aplicación también permite el almacenamiento de las consultas. El fin de esta funcionalidad es la de poder almacenar consultas en las que se invierte una cantidad considerable de tiempo para configurarlas y posteriormente poder utilizarlas en distintas ejecuciones de la herramienta. Para ello se utilizan los botones del menú "*File*" el cual permite abrir, guardar y borrar una consulta avanzada.

- **Guardar una consulta avanzada**: Pulsando el botón "*Save Advanced Query*" se permite el almacenamiento permanente de una consulta. Aparece una ventana de diálogo donde se introduce el nombre que se desea poner a la consulta a almacenar (debe ser único). Si se utiliza un nombre de una consulta existente la herramienta avisará al usuario de esa situación y pedirá confirmación para la sobre escritura de la existente. Cabe destacar que para almacenar una consulta avanzada no tiene por qué estar totalmente configurada. La consulta será almacenada en la base de datos para el proyecto que esté seleccionado.

- **Apertura de una consulta avanzada almacenada**: Para abrir una consulta guardada hay que pulsar el botón "*Open Advanced Query*" el cual hace que se muestre una ventana con una lista de las consultas almacenadas para el proyecto seleccionado.

- **Borrar una consulta almacenada**: Al pulsar sobre el botón "*Delete Advanced Query*" se abrirá una ventana con la lista de las consultas almacenadas para el proyecto seleccionado. Antes de su borrado final de

la base de datos de la aplicación se pedirá confirmación al usuario. Una vez borrada una consulta es irrecuperable.

A.2.5. Geoposicionamiento

Al igual que con el tratamiento de imágenes individual existe una funcionalidad que permite el tratamiento de la información de geoposicionamiento para las imágenes de un proyecto. Ésta se encuentra en el botón "*GPS position of project files*" del menú "*GPS operations*". Una vez pulsado este botón se abre una ventana como la de la figura 48 con las siguientes partes:

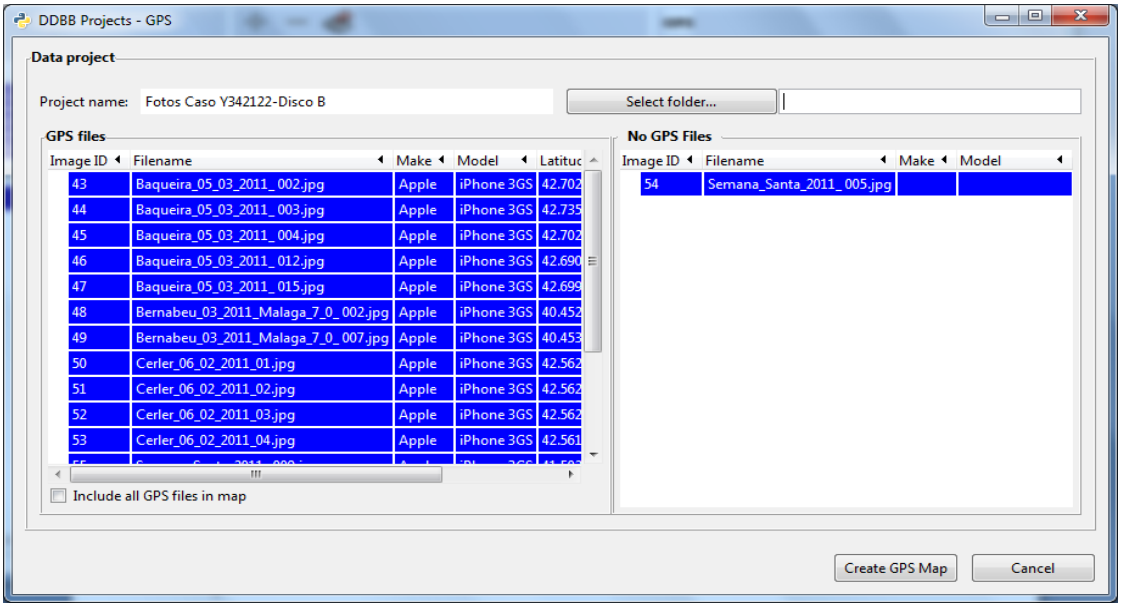


Fig. 48. Geoposicionamiento

- **Nombre del proyecto actual**: Campo no editable.

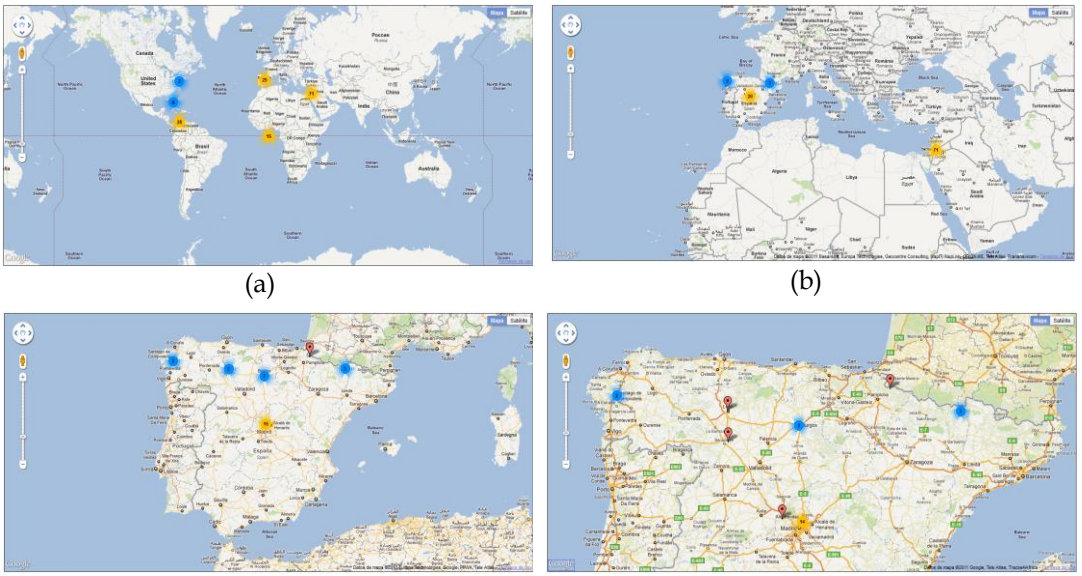
- **Lista de imágenes con información GPS de latitud y longitud**: De esta lista el usuario podrá seleccionar las imágenes que se quieren que sean ubicadas en el mapa. Si se quiere que sean todas las del proyecto seleccionar la opción "*Include all GPS files in map*".

- **Lista de imágenes sin información GPS de latitud y longitud**: Sólo se muestran a nivel informativo para que el usuario sea consciente y pueda

ver las imágenes que no pueden ser ubicadas en el mapa por no tener suficiente información de geoposicionamiento.

- **Selección de ruta donde se almacenarán los archivos de los mapas**: Es obligatorio que se seleccione una ruta donde almacenar físicamente los archivos de los mapas a generar. Esto permite que se puedan crear varios mapas con distintas imágenes de un mismo proyecto. Además permite portar los archivos y poder ser visualizados sin la herramienta. En la carpeta seleccionada se guardarán dos archivos auxiliares (data.json y markerclusterer.js) y un archivo HTML (gpsPhotos.html) el cual será el que se debe abrir con un navegador web para mostrar el mapa. Para la visualización del mapa es necesario tener conexión a Internet.

- **Botón "*Create GPS Map*"**: Al pulsar este botón y estar configurados correctamente todos los parámetros anteriormente citados se crearán los archivos del mapa en la ruta especificada y se lanzará la visualización del mapa en el navegador por defecto. En el mapa se agrupan las fotos por zona, y a medida que se aumenta el zoom se va detallando las coordenadas. La figura 49 muestra un ejemplo del mapa generado y el proceso de aumento del zoom en una zona concreta (desde la figura (a) hasta la figura (d)).



(a) (b)

(c) (d)

Fig. 49. Geoposicionamiento de un grupo de imágenes en Google Maps

A.3. Diseño e implementación de la herramienta

Como aspectos relevantes de la implementación cabe señalar las diversas herramientas utilizadas para llevar a cabo la construcción de los distintos elementos que forman la aplicación:

- El lenguaje de programación utilizado para la codificación de la aplicación es Python 2.6. De éste se destaca la utilización de la librería PIL (Python Imaging Library) que facilita diversos tipos de tratamientos sobre imágenes. El código fuente está estructurado en 5 paquetes:

  - Paquete Exif: Es el corazón de la extracción de metadatos Exif de la aplicación. Se compone de 3 clases y un conjunto de estructuras de datos auxiliares que permiten la obtención de forma eficiente de los metadatos Exif hasta la versión 2.3. Posee 1023 líneas de código.

  - Paquete BBDD: En este paquete se encuentra todo el código relativo al control de la base de datos. Se compone de 3 clases y 2059 líneas de código.

- Paquete Interface: Se encarga de controlar el flujo principal de la aplicación y todo el interface de la misma. Se compone de 15 clases y 5168 líneas de código.

- Paquete GPS: Aporta toda la funcionalidad relacionada con el geoposicionamiento de las imágenes. Se compone de 2 clases y 1384 líneas de código.

- Paquete Exception: Contiene el conjunto de clases para controlar de manera más adecuada las excepciones de la aplicación. Se compone de 3 clases y 72 líneas de código.

- Se ha utilizado como plataforma de programación Eclipse Helios, ya que permite crear entornos integrados de desarrollo multilenguaje y adaptables. Ofrece una extensa flexibilidad de configuración con los complementos necesarios para adaptar los requerimientos de desarrollo que no estén contemplados dentro de las configuraciones básicas. Para este caso concreto se requirió el uso del complemento *Pydev* de Eclipse para permitir el desarrollo en *Python*.

- Para el diseño de cada unos de los formularios de las ventanas de la aplicación se ha utilizado *Glade 3*. Esta herramienta de desarrollo visual de interfaces gráficas se basa en el uso de las librerías gráficas de *Gtk/Gnome* (en este caso *pygtk*) y genera ficheros con extensión ".glade".

- Para la lectura y posterior ejecución de las interfaces de los ficheros en formato ".glade" por código *Python* se ha utilizado el paquete Tepache.py. Tepache crea automáticamente un esquema de la clase en código *Python* que permite el control y ejecución de la interfaz generada por *Glade 3*.

- Para la realización de la documentación interna del proyecto se ha utilizado *Doxygen*.

- La gestión de versiones de todos los archivos generados en el proyecto se realiza con *Subversion*.

- El motor de base de datos utilizado es *MySQL*. En ella se almacenará toda la información necesaria para el funcionamiento de la aplicación. Las tablas que conforman la base de datos se han organizado en 4 grupos: tablas de configuración, tablas de generación de consultas, tablas de binarios de las imágenes y tablas de información Exif. En la figura 50 se presenta el modelo entidad – relación resultante del diseño de la base de datos.

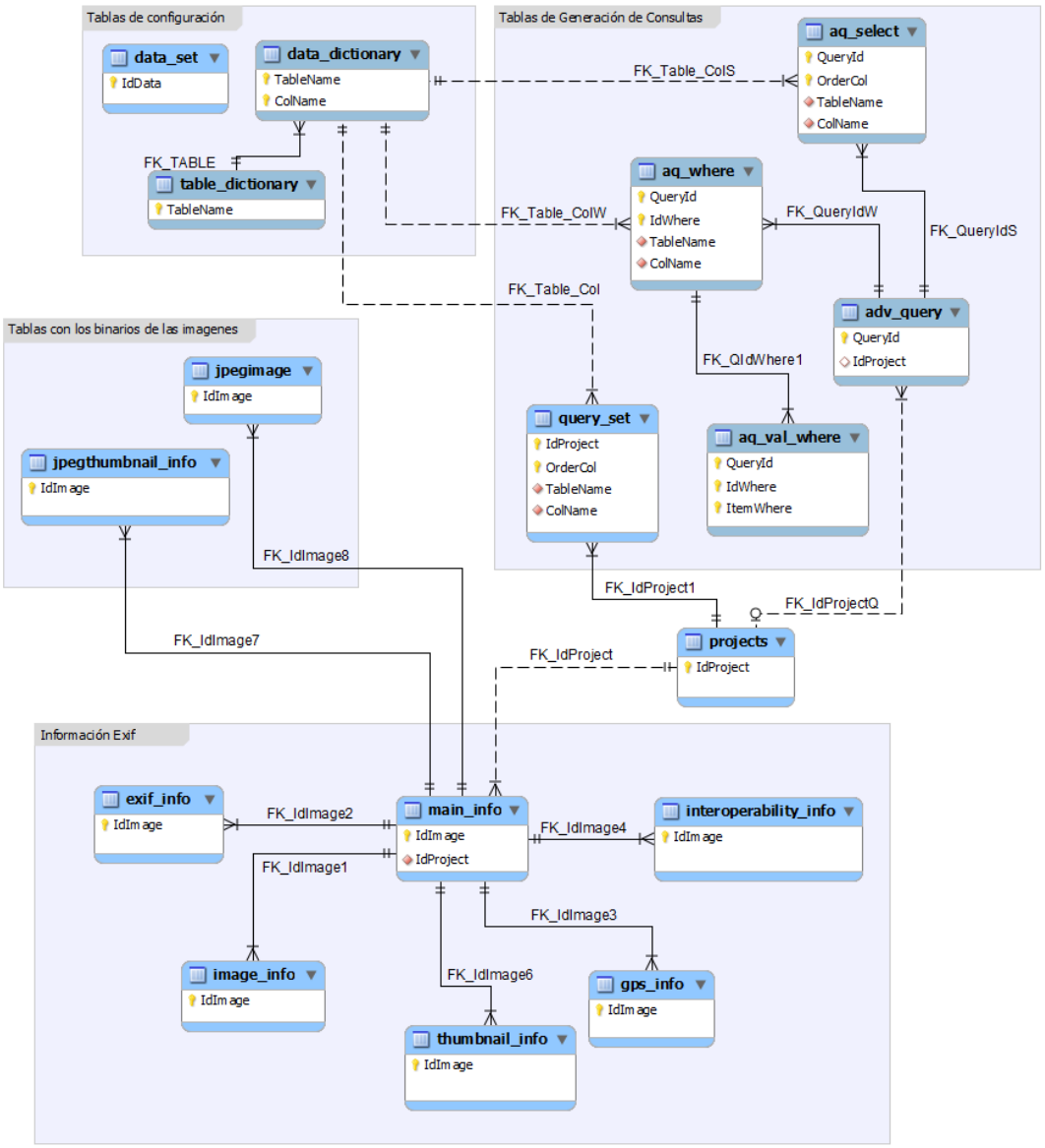


Fig. 50. Diagrama de entidad – relación de la base de datos.

A continuación se realiza una breve descripción de las tablas de los 4 grupos que conforman la base de datos:

- Tablas de configuración: Este grupo de tablas se utiliza para almacenar los parámetros generales que permiten el correcto funcionamiento de la aplicación (ver tabla 11).

Tabla	Descripción
Data_Set	Almacena los parámetros de configuración de la aplicación
Data_Dictionary	Almacenan cada una de las columnas de las tablas que conforman la base de datos.
Table_Dictionary	Almacena las tablas que conforman la base de datos.

Tabla 11. Tablas de Configuración

- Tablas de generación de consultas: Este grupo de tablas se utiliza para almacenar la configuración de las consultas que se pueden realizar sobre las imágenes almacenadas en la base de datos (ver tabla 12).

Tabla	Descripción
Query_Set	Almacena las columnas en las que se agruparán las fotografías para mostrar una información resumen.
Adv_Query	Almacena la información general de las consultas avanzadas que se pueden realizar sobre las fotografías almacenadas en la base de datos.
AQ_Select	Almacena las columnas que van a ser parte del SELECT de las consultas avanzadas.
AQ_Where	Almacena las columnas que van a ser parte del WHERE de las consultas avanzadas.
AQ_Val_Where	Almacenan los valores de las columnas que van a ser parte del WHERE de las consultas avanzadas.

Tabla 12. Tablas de generación de consultas

- Tablas de información Exif: Este grupo de tablas se utiliza para almacenar

toda la información Exif existente en la fotografía. Como puede observarse tiene estrecha relación con los distintos grupos en los que la aplicación presenta la información Exif (ver tabla 13).

Tabla	Descripción
Main_Info	Almacena información general sobre la fotografía, incluyendo información general del fichero como tal, y un resumen de la información EXIF presente en la misma.
Image_Info	Almacena información de los datos del IFD de imagen.
Thumbnail_Info	Almacena información de los datos del IFD de thumbnail.
Exif_Info	Almacena información de los datos del IFD de EXIF.
GPS_Info	Almacena información de georeferenciación de las fotos.
Interoperability_Info	Almacena información de los datos del IFD de Interoperabilidad.

Tabla 13. Tablas de información Exif